Yamhill County Health and Human Services

Health Insurance Portability, and Accountability Act (HIPAA) and 42 Code of Federal Regulations (CFR) Part 2 Manual

Policy Numbers: 016-79-09-00 to 016-79-09-11

Approved: _____

Lindsey Manfrin, Director

Yamhill County Health and Human Services

Date revised: April 22, 2022

Preamble:

The following manual addresses the key requirements of the HIPAA Privacy and Security Rule. In addition, where there is a stricter standard, such as with 42 CFR Part 2, *Confidentiality of Alcohol and Drug Abuse Patient Records*, the stricter standard will be noted and shall be followed.

Table of Contents

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Client Rights

POLICY NUMBER: 016-79-09-01

Table of Contents:

1. PURPOSE

The intent of this policy is to establish the privacy rights that Yamhill County Health and Human Services (YCHHS) clients have regarding the use and disclosure of their protected information that is held by YCHHS, and to describe the process for filing a complaint should clients feel those rights have been violated.

2. TERMS

- ***Client:*** An Individual who requests or receives services from YCHHS.
- ***Client Records:*** All personal information that YCHHS has collected, compiled, or created about YCHHS clients, which YCHHS may maintain in one or more locations and in various forms, reports, or documents, including information that is stored or transmitted by electronic media.
- ***Designated Record Set (§164.501(1):***
  - A group of records maintained by or for YCHHS that is:
    a. The medical records and billing records concerning individuals maintained by or for YCHHS;
    b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for YCHHS; or
    c. Used, in whole or in part, by or for YCHHS to make decisions about individuals.
      - For purposes of this definition, "record" means:
    d. Any item, collection or grouping of information that includes protected health information; and
    e. Is maintained, collected, used, or disseminated by or for YCHHS;
- ***Individually Identifying Information (§160.103):*** Any single item or compilation of information or data that is a subset of health information (such as the individual's name or social security number), and:
    1. Is created or received by YCHHS; and
    2. Relates to the past, present or future physical or mental or substance use 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
        a. That identifies the individual; or
        b. A reasonable basis to believe the information can be used to identify the individual.
    3. **Behavioral Health Only** (42 CFR Part 2: Information (§2.12):
        a. That would identify a client as having or having had a substance use disorder either directly, by reference to other publicly available information, or through verification of such an identification by another person.
        b. Obtained for the purpose of treating a substance use disorder, making a diagnosis for the treatment, or making a referral for that treatment.
- ***Minimum Necessary (§164.502):*** The least amount of information, when using or disclosing confidential client information that is needed to accomplish the intended purpose of the use, disclosure, or request.
- ***Protected Health Information (PHI) (§164.103):*** Any "individually identifying health information" (see definition above), whether oral or recorded, that is:
  1. Transmitted by electronic media;

2. Maintained in electronic media;
3. Transmitted or maintained in any other form or medium.

- ***Psychotherapy Notes (§164.501)***: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.

Please note by HIPAA definition that:

1. *Psychotherapy notes* are not the same as the YCHHS service note. They are very distinct, as noted above, and do not include such things as: medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the service plan, symptoms, prognosis, service notes, and progress to date; and
2. *Psychotherapy notes* are personal notes recorded by the clinician, and by definition, not intended for others; and
3. *Psychotherapy notes* should not be retained in the YCHHS electronic health record or the client's physical chart.

3. GENERAL PROCEDURES

A. **YCHHS clients have the right to, and YCHHS may not deny, the following (§164.528):**

A.1. Access to their own information, consistent with certain limitations;

A.2. Receive an accounting of disclosures YCHHS has made of their protected health information (PHI) for up to six years prior to the date of requesting such accounting. Information may not be available prior to the effective date of this policy (March 31, 2003) and certain limitations do apply as outlined in this policy, section 6; and

A.3. Submit complaints if they believe or suspect that information about them has been improperly used or disclosed, or if they have concerns about the privacy policies of YCHHS. (§164.520)

B. **Clients Rights to Take Action on their PHI (§164.522):**

B.1. Clients may ask YCHHS to take specific actions regarding the use and disclosure of their information and YCHHS may either approve or deny the request. Specifically, clients have the right to request:

B.1.1. That YCHHS restrict uses and disclosures of their individual information while carrying out treatment, payment activities, or health care operations;

B.1.2. To receive information from YCHHS by alternative means, such as mail, fax or telephone, or at alternative locations; and

a) For electronic communication, see YCHHS Policy 016-79-03-02, *Electronic Communication With or About Clients* and *Electronic Communication Use and Consent* Form.

B.1.3. That YCHHS amend their information that is held by YCHHS.

C. **Relationship to Notice of Privacy Practices (§164.520):**

C.1. YCHHS will use the *YCHHS Notice of Privacy*, to inform clients about how YCHHS may use and/or disclose their information. The *Notice of Privacy* also describes the actions a client may take, or request YCHHS to take, with regard to the use and/or disclosure of their information.

C.2. Nothing in this policy, or the policy related to the YCHHS *Notice of Privacy*, shall prevent YCHHS from changing its policies or the *Notice* at any time, provided that the changes in the policies or *Notice* comply with state or federal law.

D. **Decision-making authority within YCHHS:**

D.1. Prior to any decision, based on a client's request for YCHHS to amend a health or medical record, the program's director or a licensed clinical staff designated by the program administrator shall review the request and any related documentation. The licensed clinical staff may be a YCHHS staff person involved in the client's case.

D.2. Prior to any decision to amend any other information, that is not a health or medical record, a YCHHS staff person, designated by the program administrator, shall review the request and any related documentation.

D.3. YCHHS may deny a client access to their own health information on the grounds that access may result in risk or harm to the client or to another person. However, prior to any decision to deny such access, the program's medical director or a licensed health care professional, designated by the program administrator, shall review the request and any related documentation. The licensed health care professional may be a YCHHS staff person involved in the client's case.

D.4. Decisions related to any other requests made to YCHHS under this policy shall be handled in a manner consistent with federal and state rules and regulations and/or YCHHS policies and procedures applicable to the program, service, or activity.

4. RESTRICTIONS OF USE AND DISCLOSURES OF PHI (§164.522)

A. **General Client Rights**:

A.1. Clients have the right to request restrictions on the use and/or disclosure of their information.

A.2. YCHHS applies confidentiality laws applicable to specific programs or activities to protect the privacy of client information. Even if those laws would permit YCHHS to make or use a disclosure of information, a YCHHS client has the right to request a restriction on a use or disclosure of that information.

A.3. All requests will be submitted by completing a YCHHS Form #1011, *Restricting Use and Disclosures Request and Amending Protected Health Information Request*.

A.4. YCHHS is not obligated to agree to a restriction and may deny the request or may agree to a restriction more limited than what the client requested.

A.4.1. **Exception:** Certain programs can only disclose information that is authorized by the client, such as alcohol and drug, mental health or certain Public Health programs. For those program participants, YCHHS will honor their requests for restriction by making sure that the authorization clearly identifies the authorized recipients of the information.

B. **Requesting Restrictions Procedure:**

B.1. Clients may request that YCHHS restrict the use and/or disclosure of their information for the purpose of:

B.1.1. Carrying out treatment, payment, or health care operations;

B.1.2. Disclosure of health information to a relative or other person who is involved in the client's care;

B.2. All requests for access will be made by having the client complete a YCHHS Form #1022, *Access to Records and Accounting of Disclosure Request* Form.

C. **YCHHS is not required to agree to a restriction requested by the client:**

C.1. YCHHS will not agree to restrict uses or disclosures of information if the restriction would adversely affect the quality of the client's care or services. (§164.510)

- **Behavioral Health Only:** Substance use disorder assessment and treatment records cannot be released except for situations that constitute an emergency as described in C.3 per 42 CFR part 2.

C.2. YCHHS cannot agree to a restriction that would limit or prevent YCHHS from making or obtaining payment for services. (§164.506)

- **Behavioral Health Only:** Substance use disorder assessment and treatment records cannot be released except for situations which constitute an emergency situation as described in c.3 per 42 CFR part 2.

C.3. Emergency treatment should be provided even with an agreed upon restriction (see "exception" under (E.1) below, of this Policy (§164.510).

a) **Behavioral Health Only:** For substance use, mental health participants or certain Public Health programs, Federal regulations (42 CFR Part 2 and 34 CFR) prohibit YCHHS from denying client requests for restrictions on uses and disclosures of their information regarding treatment or rehabilitation.

D. **Documentation (§164.522(a)(3) and §164.530(j):**

D.1. YCHHS will document the client's request, and the reasons for granting or denying the request in the client's YCHHS hard copy or electronic case record file.

D.1.1. Prior to any use of disclosure of client information, YCHHS staff must confirm that such use or disclosure has not been granted a restriction by reviewing the client's case file.

E. **If YCHHS Agrees with the Request:**

E.1. If YCHHS agrees to a client's request for restriction, YCHHS will not use or disclose information that violates the restriction.

a) **Exception:** If the client needs emergency treatment and the restricted information is needed to provide emergency treatment, YCHHS may use or disclose such information to the extent needed to provide the emergency treatment. However, once the emergency situation subsides YCHHS must ask the provider not to re-disclose the information.

F. **YCHHS may terminate its agreement to a restriction if:**

F.1. The client agrees to or requests termination of the restriction in writing;

F.2. The client orally agrees to, or requests termination of the restriction. YCHHS will document the oral agreement or request in the client's YCHHS case record file; or

F.3. YCHHS informs the client in writing that YCHHS is terminating its agreement to the restriction. Information created or received while the restriction was in effect shall remain subject to the restriction.

5. ALTERNATIVE MEANS OR LOCATION FOR COMMUNICATION (§164.522)

A. **General Client Rights**:

A.1. YCHHS must accommodate reasonable requests by clients to receive communications by alternative means, such as by mail, e-mail, fax or telephone; and

A.2. YCHHS must accommodate reasonable requests by clients to receive communications at an alternative location.

A.3. In some cases, sensitive health information or health services must be handled with strict confidentiality under state law. For example, information about substance use disorder treatment may be subject to specific handling. YCHHS will comply with the more restrictive requirements.

A.3.1. For electronic communication, see YCHHS policy #016-79-03-02, *Electronic Communication With or About Client* and *Electronic Communication Use and Consent* Form.

B. **Requesting Process:**

B.1. The client must specify the preferred alternative means or location.

B.2. Requests for alternative means or alternative locations for information may be made orally or in writing.

C. **Documentation:**

C.1. If a client makes a request orally, YCHHS will document the request and ask for the client's signature.

C.2. If a client makes a request by telephone or electronically, YCHHS will document the request in the client record and verify the identity of the requestor.

D. **Verification:**

D.1. Prior to any information being sent to the client, YCHHS staff must confirm if the client has requested an alternate location or by alternate means, and if YCHHS has granted that request, by reviewing the client's case file.

E. **Denial or Termination of Alternative Communication (OAR 407-014-0030(4)(c):**

E.1. YCHHS may terminate its agreement to an alternative location or method of communication if:

E.1.1. The client agrees to or requests termination of the alternative location or method of communication in writing or orally. YCHHS will document the oral agreement or request in the client's YCHHS case record file.

E.1.2. YCHHS informs the client that YCHHS is terminating its agreement to the alternative location or method of communication because the alternative location or method of communication is not effective. YCHHS may terminate its agreement to communicate at the alternate location or by the alternative means if:

a) YCHHS is unable to contact the client at the location or in the manner requested; or

b) If the client fails to respond to payment requests if applicable.

6. REQUESTING ACCESS TO INFORMATION (§164.524 AND 42 CFR PART 2 (§2.23)

A. **General Client Rights:**

A.1. YCHHS will assure that clients may access their information that YCHHS uses in whole or part to make decisions about them, subject to certain limitations as outlined in this section of Policy.

A.2. Clients have the right to access, inspect, and obtain a copy of information from their own Designated Record Set in YCHHS files or records, consistent with federal law and the Oregon Public Records Law.

A.2.1. All requests for access will be made having the client complete a YCHHS Form #1022, *Access to Records and Accounting of Disclosures Request Form*.

A.3. Under federal law, clients have the right to access, inspect, and obtain a copy of health information on their own cases in YCHHS files or records **except for**:

A.3.1. Information compiled for use in civil, criminal, or administrative proceedings;

A.3.2. Information that is subject to the federal Clinical Labs Improvement Amendments of 1988, or exempt pursuant to 42 CFR 493.3(a)(2);

A.3.3. Information that, in good faith, YCHHS believes can cause harm to the client, participant or to any other person (see B. of this Section);

A.3.4. Documents protected by attorney work-product privilege; and

A.3.5. Information where release is prohibited by State or Federal Laws.

B. **Requesting Access to PHI**:

Before YCHHS denies a client access to their information because there is a good faith belief that its disclosure could cause harm to the client or to another person, the YCHHS decision to deny must be made by a licensed health care professional or other designated staff, and YCHHS must make a review of this denial available to the client. If the client wishes to have this denial reviewed, a licensed health care professional who was not involved in the original decision must do the review**.**

B.1. Clients may request access to their own information that is kept by YCHHS by using a personal identifier (such as the client's name or YCHHS case number).

B.1.1. If YCHHS maintains information about the client in a record that includes information about other people, the client is only authorized to see information about themselves, except as provided below:

B.1.2. If the person requesting information is recognized under Oregon law as a guardian or legal custodian of the client and is authorized by Oregon law to have access to the client's information or to act on behalf of the client for making decisions about the client's services or care, YCHHS will release information to the requestor.

B.1.3. Access to records of Individual with disability or individual with mental illness: "The system designated to protect and advocate for the rights of individuals [with developmental disabilities or mental illness] shall have access to all records" per ORS 192.517 (1), and under part C of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 15043) and the rights of individuals with mental illness under the Protection and Advocacy for Individuals with Mental Illness Act (42 U.S.C. 10806), shall have access to all records, as defined in ORS 192.515, and as provided in ORS 192.517.

C. **YCHHS may Deny Access, Unreviewable, if (§164.524(1)(2):**

C.1. Psychotherapy notes (see *Client Rights*, Section 2 for definition), or

C.2. Information compiled in reasonable anticipation, or for use in, a civil, criminal, or administrative action or proceeding; and

C.3. Protected health information maintained by a covered entity that is:

C.3.1. Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a; or

C.3.2. Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2)

C.4. Was obtained from someone other than a health care provider under a promise of confidentiality, and access would reveal the source of the information.

D. **YCHHS may Deny Clients Access with a Review, in the following circumstances (§164.524(3):**

D.1. A licensed health care professional or other designated staff has determined, in the exercise of professional judgment, that the information requested may endanger the life or physical safety of the client or another person; or

D.2. The protected information makes reference to another person, and a licensed health care professional or other designated staff has determined, in the exercise of professional judgment, that the information requested may cause substantial harm to the client or another person; or

D.3. The request for access is made by the client's personal representative, and a licensed health care professional or other designated staff has determined, in the exercise of professional judgment, that allowing the personal representative to access the information may cause substantial harm to the client or to another person.

E. **Client Request for a Review:**

E.1. If YCHHS denies access under Section 6.D. of this Policy (above), the client has the right to have the decision reviewed by a licensed health care professional or other designated staff not directly involved in making the original denial decision. YCHHS will then proceed based on the decision from this review.

E.1.1. YCHHS must promptly refer a request for review to the designated reviewer. [See Section (6.)(F.) below of this Policy for timelines for these procedures].

E.1.2. The reviewer must determine, within a reasonable time, whether or not to approve or deny the client's request for access, in accordance with this policy.

E.1.3. YCHHS must then:

a) Promptly notify the client in writing of the reviewer's determination; and

b) Take action to carry out the reviewer's determination.

F. **Timing and Response by YCHHS:**

F.1. YCHHS must act on a client's request for access no later than 30 days after receiving the request, except in the case of written accounts under ORS 179.505 which must be disclosed within five (5) days.

F.1.1. In cases where the information is not maintained or accessible to YCHHS on-site, and does not fall under ORS 179.505, YCHHS must act on the client's request no later than 60 days after receiving the request.

F.1.2. If YCHHS is unable to act within these 30-day or 60-day limits, YCHHS may extend this limitation by up to an additional 30 days, subject to the following:

a) YCHHS must notify the client in writing of the reasons for the delay and the date by which YCHHS will act on the request.

b) YCHHS will use only one such 30-day extension to act on a request for access.

G. **If Request is Granted:**

G.1. If YCHHS grants the client's request, in whole or in part, YCHHS must inform the client of the access decision and provide the requested access.

G.1.1. If YCHHS maintains the same information in more than one format (such as electronically and in a hard-copy file) or at more than one location, YCHHS need only provide the requested protected information once.

G.1.2. YCHHS must provide the requested information in a form or format requested by the client, if readily producible in that form or format. If not readily producible, YCHHS will provide the information in a readable hard-copy format or such other format as agreed to by YCHHS and the client.

G.1.3. If YCHHS does not maintain, in whole or in part, the requested information, and knows where the information is maintained, YCHHS will inform the client of where to request access.

G.1.4. YCHHS may provide the client with a summary of the requested information, in lieu of providing access, or may provide an explanation of the information if access had been provided, if:

a) The client agrees in advance; and

b) The client agrees in advance to any fees YCHHS may impose, per Subsection (6.)(G.1.6.) of this Policy, below.

G.1.5. YCHHS must arrange with the client for providing the requested access in a time and place convenient for the client and YCHHS. This may include mailing the information to the client if the client so requests or agrees.

G.1.6. Fees (§164.524(c)(4): A client (or personal representative or legal guardian or custodian) may request a copy of their information at no cost once every 12 months. If the client requests a copy of the requested information, or a written summary or explanation, more frequently than once every 12

months, then YCHHS may impose its Usual & Customary charge for the following:

a) Copying the requested information or saving the information to electronic media, including the costs of supplies and of the labor of copying;

b) Postage, when the client has requested or agreed to having the information mailed; and

c) Preparing an explanation or summary of the requested information, if agreed to in advance by the client, per Subsection (6.)(G.1.4.) of this Policy, above.

G.1.7. The individual is entitled to one free records request for the appeal of a Social Security benefit denial per ORS 192.576.

H. **If YCHHS Denies Access:**

H.1. If YCHHS denies access, in whole or in part, to the requested information, YCHHS must:

H.1.1. Give the client access to any other requested client information after excluding the information to which access is denied;

H.1.2. Provide the client with a timely written denial. The denial must:

a) Be sent or provided within the time limits specified in Section (6)(F.) of this Policy, above;

b) State the basis for the denial, in plain language;

c) If the reason for the denial is due to danger to the client or another, explain the client's review rights as specified in Section (6.)(E.) of this Policy, above, including an explanation of how the client may exercise these rights; and

d) Provide a description of how the client may file a complaint with YCHHS, and if the information denied is protected health information, with the United States Department of Health and Human Services (DHHS)-Office of Civil Rights, pursuant to Section (9.) of this Policy, below.

1) The description must include the name, or title, and telephone number of the contact person or designated office.

H.1.3. If YCHHS does not maintain the requested protected information and knows where such information is maintained (such as by a medical provider, insurer, other public agency, private business, or other non-YCHHS entity), YCHHS must inform the client of where to direct the request for access.

7. REQUESTING AMENDMENTS OF PROTECTED HEALTH INFORMATION (§164.526)

A. **General Client Rights:**

A.1 Clients have the right to request that YCHHS amend their information in the YCHHS designated record set for as long as the protected health information is maintained in the designated record set.

A.2 All requests for amendments will be made by having the client complete the YCHHS Form #1011, *Restricting Use and Disclosure and Amending Protected Health Record Information Request*.

A.3 YCHHS is not obligated to agree to an amendment and may deny the requests or limit its agreement to amend.

A.4 YCHHS will honor requests for alternative methods of making this request if reasonable accommodations are needed.

B. **Timing and Response by YCHHS:**

B.1. YCHHS must act on the client's request no later than 60 days after receiving the request. If YCHHS is unable to act on the request within 60 days, YCHHS may extend this time limit by up to an additional 30 days, subject to the following:

B.1.1. YCHHS must notify the client in writing of the reasons for the delay and the date by which YCHHS will act on the receipt; and

B.1.2. YCHHS will use only one such 30-day extension.

C. **If YCHHS Accepts the Amendment:**

C.1. If the request is accepted, in whole or in part, YCHHS must:

C.1.1. Make the appropriate amendment to the protected information or records, and document the amendment in the client's designated record set;

C.1.2. Provide timely notice to the client that the amendment has been accepted no later than 60 days after receiving the request;

C.1.3. Seek the client's agreement to notify other relevant persons or entities, with whom YCHHS has shared or needs to share the amended information, of the amendment; and

C.1.4. Make reasonable efforts to inform, and to provide the amendment within a reasonable time to:

a) Persons named by the client as having received protected health information and who thus need the amendment; and

b) Persons, including business associates of YCHHS, that YCHHS knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on the information to the client's detriment.

C.2. Prior to any decision to amend a health or medical record, the request and any related documentation shall be reviewed by the program's medical director, a licensed health care professional designated by the program administrator, or a YCHHS staff person involved in the client's case.

C.3. Prior to any decision to amend any other information, that is not a health or medical record, a YCHHS staff person designated by the program administrator shall review the request and any related documentation.

D. **YCHHS may deny the client's request for amendment if:**

D.1. YCHHS finds the information to be accurate and complete;

D.2. The information was not created by YCHHS, unless the client provides a reasonable basis to believe that the originator of such information is no longer available to act on the requested amendment;

D.3. The information is not part of YCHHS designated record set; or

D.4. If it would not be available for inspection or access by the client, pursuant to Section (6.)(C-D) of this Policy.

E. **If YCHHS denies the requested amendment, in whole or in part, YCHHS must:**

E.1. Provide the client with a timely written denial. The denial must:

E.1.1. Be sent or provided within 60 days of receiving the request.

E.1.2. State the basis for the denial, in plain language;

E.1.3. Explain the client's right to submit a written statement disagreeing with the denial and how to file such a statement. If the client does so:

a) YCHHS will enter the written statement into the client's YCHHS designated record set;

b) YCHHS may also enter a YCHHS written rebuttal of the client's written statement into the client's YCHHS designated record set. YCHHS will send or provide a copy of any such written rebuttal to the client;

c) YCHHS will include a copy of that statement, and of the written rebuttal by YCHHS if any, with any future disclosures of the relevant information; and

d) Explain that if the client does not submit a written statement of disagreement, the client may ask that if YCHHS makes any future disclosures of the relevant information, YCHHS will also include a copy of the client's original request for amendment and a copy of the YCHHS written denial; and

e) Provide information on how the client may file a complaint with YCHHS, or with the U.S. Department of Health and Human Services (DHHS), Office of Civil Rights, subject to Section (9.) of this Policy, below.

8. REQUESTING AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

F. **General Clients Rights:**

F.1. Clients have the right to receive an accounting of disclosures of protected health information (PHI) that YCHHS has made for any period of time, not to

exceed six years, preceding the date of requesting the accounting (§164.528 and 42 CFR Part 2, §2.13(d).

F.2. The accounting will only include health information NOT previously authorized by the client for use or disclosure, and will not include information collected, used, or disclosed for treatment, payment or health care operations for that client.

F.3. All requests for amendments will be made by having the client complete a YCHHS Form #1022, *Accounting of Disclosures Request Form*.

F.4. This right does not apply to disclosures made prior to the effective date of this Policy, which is March 31, 2003.

G. **Example of disclosures of PHI that are required to be listed in an accounting:**

G.1. **Abuse Report:** PHI about an individual provided by YCHHS staff (other than protective services staff who respond to such report) pursuant to mandatory abuse reporting laws to an entity authorized by law to receive the abuse report.

G.2. **Audit Review:** PHI provided by YCHHS staff from an individual's record in relation to an audit or review (whether financial or quality of care or other audit or review) of a provider or contractor.

G.3. **Health and Safety:** PHI about an individual provided by YCHHS staff to avert a serious threat to health or safety of a person.

G.4. **Licensee/Provider:** PHI provided by YCHHS from an individual's records in relation to licensing or regulation or certification of a provider or licensee or entity involved in the care or services of the individual.

G.5. **Legal Proceeding:** PHI about an individual that is ordered to be disclosed pursuant to a court order in a court case or other legal proceeding – include a copy of the court order with the accounting.

G.6. **Law Enforcement Official/Court Order:** PHI about an individual provided to a law enforcement official pursuant to a court order – include a copy of the court order with the accounting.

G.7. **Law Enforcement Official/Deceased:** PHI provided to law enforcement officials or medical examiner about a person who has died for the purpose of identifying the deceased person, determining cause of death, or as otherwise authorized by law.

G.8. **Law Enforcement Official/Warrant:** PHI provided to a law enforcement official in relation to a fleeing felon or for whom a warrant for their arrest has been issued and the law enforcement official has made proper request for the information, to the extent otherwise permitted by law.

G.9. **Media:** PHI provided to the media (TV, newspaper, etc.) that is not within the scope of an authorization by the individual.

G.10. **Public Health Official:** PHI about an individual provided by YCHHS staff (other than staff employed for public health functions) to a public health

official, such as the reporting of disease, injury, or the conduct of a public health study or investigation.

G.11. **Public Record:** PHI about an individual that is disclosed pursuant to a Public Record request without the individual's authorization.

G.12. **Research:** PHI about an individual provided by YCHHS staff for purposes of research conducted without authorization. A copy of the research protocol should be kept with the accounting, along with the other information required under the HIPAA privacy rule, 45 CFR § 164.528(b)(4).

H. **Disclosures that are not required to be tracked (See more stringent requirements below for disclosures of SUD PHI under H.10 Behavioral Health Only, below):**

H.1. Made prior to the original effective date of this original policy, which is March 31, 2003;

H.2. Disclosures made for treatment, payment, and healthcare operation purposes (§164.502);

H.3. Disclosures made to the individual (§164.502);

H.4. Disclosures pursuant to an authorization (§164.528);

H.5. Disclosures made for directory purposes (§164.510);

H.6. Disclosures made to persons involved in the individual's care (§164.510);

H.7. Disclosures made for national security or intelligence purposes (§164.512(k)(5));

H.8. Disclosures to correctional institutions or law enforcement officials (§164.512(k)(5);

H.9. Made as part of a limited data set in accordance with the YCHHS policy #016-79-09-05: *De-identification of Client Information and Use of Limited Data Sets*.

H.10. **Behavioral Health Only (42 CFR Part 2, §2.13(d)**:

H.10.1. List of disclosures. Upon request, patients who have consented to disclose their patient identifying information using a general designation pursuant to §2.31(a)(4)(iii)(B) must be provided a list of entities to which their information has been disclosed pursuant to the general designation.

H.10.2. Under this paragraph, patient requests:

a) Must be made in writing; and

b) Are limited to disclosures made within the past two years;

H.10.3. Under this paragraph, the entity named on the consent form that discloses information pursuant to a patient's general designation (the entity that serves as an intermediary, as described in §2.31(a)(4)(iii)(B) must:

a) Respond in 30 or fewer days of receipt of the written request; and

b) See Section I. *The accounting must include, for each disclosure* below.

I. **The accounting must include, for each disclosure:**

I.1. The date of the disclosure;

I.2. The name, and address if known, of the person or entity(ies) who received the disclosed information;

I.3. A brief description of the information disclosed; and

I.4. A brief statement of the purpose of the disclosure that reasonably informs the client of the basis for the disclosure, or, in lieu of such statement, a copy of the client's written request for a disclosure, if any.

J. **Multiple Disclosure exception:**

J.1. If, during the time period covered by the accounting, YCHHS has made multiple disclosures to the same person or entity for the same purpose, or as a result of a single written authorization by the client; YCHHS may provide:

J.1.1. Although YCHHS must provide a written accounting for disclosures made over a six-year period, only the first disclosure made during the time period is necessary (YCHHS need not list the same identical information for each subsequent disclosure to the same person or entity) if YCHHS adds:

a) The frequency or number of disclosures made to the same person or entity;

b) The last date of the disclosure made during the requested time period.

K. **Timing and Response to Individual's Request for Accounting:**

K.1. YCHHS must act on the client's request for an accounting no later than 60 days after receiving the request, subject to the following:

K.1.1. If unable to provide the accounting within 60 days after receiving the request, YCHHS may extend this requirement by another 30 days. YCHHS must provide the client with a written statement of the reasons for the delay within the original 60-day limit and inform the client of the date by which YCHHS will provide the accounting.

K.1.2. YCHHS will use only one such 30-day extension.

L. **Fee for Accounting (164.528(c)(2):**

L.1. YCHHS must provide the first requested accounting in any 12-month period without charge.

L.1.1. If the client requests an accounting of disclosures subsequent to the first request within the 12-month period, then YCHHS may impose its reason based Usual & Customary charge for the following:

a) Copying the requested information, including the costs of supplies and of the labor of copying;

b) Postage, when the client has requested or agreed to having the information mailed; and

c) Preparing an explanation or summary of the requested information, if agreed to in advance by the client, per subsection (6)(G.1.4.) of this Policy, above.

L.1.2. Informs the client of the fee before proceeding with any such additional request; and

L.1.3. Allows the client an opportunity to withdraw or modify the request in order to avoid or reduce the fee or seek a variance from the HHS Division manager.

M. **Documentation for client file:**

M.1. YCHHS must:

M.1.1. Document, and retain in the client's YCHHS case record for 6 years from the date of its creation or the date when it last was in effect, whichever is later, the information required to be included in an accounting of disclosures, as listed under Section (8.)(D.) of this Policy, and

M.1.2. Send a copy of the written accounting provided to the client.

N. **Required Exceptions:**

N.1. YCHHS will temporarily suspend a client's right to receive an accounting of disclosures that YCHHS has made to a health oversight agency or to a law enforcement official, for a length of time specified by such agency or official, if:

N.1.1. The agency or official provides a written statement to YCHHS that such an accounting would be reasonably likely to impede their activities and specify the time for which such a suspension is required.

N.1.2. However, if such agency or official makes an **oral** request, YCHHS will:

a) Document the oral request, including the identity of the agency or official making the request;

b) Temporarily suspend the client's right to an accounting of disclosures pursuant to the request; and

c) Limit the temporary suspension to no longer than 30 days from the date of the oral request, unless the agency or official submits a written request specifying a longer time period.

9. RIGHTS OF CLIENTS TO FILE COMPLAINTS REGARDING DISCLOSURE OF INFORMATION (§164.520 §164.530(D)(1)

A. **General Clients Rights:**

A.1. Clients have a right to submit a complaint if they believe that YCHHS has improperly used or disclosed their protected information, or if they have concerns about the privacy policies of YCHHS or concerns about YCHHS compliance with such policies.

A.2. YCHHS will not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person filing a complaint or inquiring about how to file a complaint.

A.3. YCHHS may not require clients to waive their rights to file a complaint as a condition of providing of treatment, payment, enrollment in a health plan, or eligibility for benefits.

B. **Filing a Complaint:**

B.1. Clients may file complaints with the YCHHS Privacy Officer per the YCHHS policy #016-79-08-03, *Complaints, Grievances and Appeals*, Oregon Department of Health and Human Services, or with the U.S. Department of Health and Human Services (DHHS) - the Office of Civil Rights. The following are where Privacy Complaints may be filed:

Yamhill County Health and Human Services	**Oregon Department of Health and Human Services**
Privacy Official: 627 NE Evans McMinnville, OR 97128 Phone: (503) 434-7404	Medical Privacy, Complaint Division 200 Independence Avenue, SW HHH Building, Room 509H Washington, D.C. 20201 Phone: 866-627-7748 TTY: 886-788-4989 Email: www.hhs.gov/ocr
Yamhill County	**U. S. Department of Health and Human Services, Office of Civil Rights:**
Privacy Officer: 525 NE 5th St. McMinnville, OR 97128	Medical Privacy, Complaint Division 200 Independence Avenue, SW Washington, D.C. 20201 Toll free Phone: 877-696-6775 Phone: 866-627-7748 TTY: 886-788-4989 Email: www.hhs.gov/ocr

C. **Review Process:**

C.1. YCHHS will designate staff to review and determine action on complaints filed with YCHHS. Designated staff will also perform these functions when YCHHS is contacted about complaints filed with the U.S. Department of Health and Human Services – the Office of Civil Rights.

D. **Documentation:**

D.1. The YCHHS Privacy Officer or designee will document all complaints, the findings from reviewing each complaint, and YCHHS actions resulting from the complaint. This documentation shall include a description of corrective actions that YCHHS has taken, if any are necessary, or of why corrective actions are not needed, for each specific complaint.

D.2. Documents will be kept for six years.

E. **Time Frame for Resolution:**

E.1. YCHHS will comply with the process and timeframe outlined in YCHHS policy #016-79-08-03, *Complaints, Grievances and Appeals*, which will include:

E.1.1. Name of a contact person who can answer any questions the client may have.

E.1.2. The date of the investigation and general description of steps taken to investigate the Privacy Complaint

E.1.3. An explanation of YCHHS' resolution.

10. PERSONAL REPRESENTATIVES OF PATIENTS (§164.502(G)(1)

A. YCHHS shall treat an individual's personal representative as the individual with respect to the Protected Health Information of the individual.

B. The personal representative of an individual is a person who, under applicable Oregon law, has the authority to act on behalf of an individual in making decisions related to health care.

B.1. The following persons are authorized under Oregon law to act as a personal representative of an individual (ORS 192.556):

B.1.1. A parent (in the case of a patient who is an unemancipated minor);

- **Exception:** Minors who are of legal age to consent to treatment must do so in the case of substance use disorder and mental health treatment (§5b.9-10; ORS 109.675).

B.1.2. A guardian appointed by a court to make health care decisions for an individual;

B.1.3. An attorney-in-fact (also known as the agent) appointed by an individual under a health care power of attorney; and

B.1.4. An unappointed health care representative in accordance with the Oregon Health Care Decisions Act or other applicable Oregon law.

C. In regards to personal representative of clients YCHHS will use the following procedures:

C.1. Verification (§5b.5(b); §164.514(h):

C.1.1. Verify that the person is qualified under Oregon Law to be a Personal Representative prior to allowing the individual access to client protected health information.

C.2. File Documentation:

C.2.1. YCHHS will maintain on file written documentation of a person's qualifications to act as an individual's personal representative.

C.3. Special Situations:

C.3.1. Unemancipated Minors: YCHHS will treat a parent, guardian or other person acting *in loco parentis*, as authorized under Oregon law, as the

personal representative of an unemancipated minor with respect to such minor's Protected Health Information. However, YCHHS will not treat such person as the minor's personal representative, with respect to accessing Protected Health Information if:

a) The minor consents to such health care service;

b) The minor may lawfully obtain health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, provided that the minor, a court, or another person authorized by law consents to such health care service; or

c) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between YCHHS and the minor with respect to such health care service.

C.3.2. Deceased Individuals: If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, YCHHS will treat such person as a personal representative with respect to Protected Health Information relevant to such personal representation. (See ORS 113.085 and 192.573)

C.3.3. Abuse, Neglect, Endangerment Situations: YCHHS may elect not to treat a person as the personal representative of an individual if:

a) YCHHS has a reasonable belief that:

1) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

2) Treating such person as the personal representative could endanger the individual;

3) YCHHS in the exercise of professional judgment decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

11. **FORMS**

- YCHHS Form: "Notice of Privacy Practices"
- YCHHS Form # 1011: "Restricting Use and Disclosures and Amending Protected Health Information Request"
- YCHHS Form #1021: "Disclosures Log/Release of Protected Health Information Tracking Log"
- YCHHS Form #1022: "Access to Records and Accounting of Disclosures Request"

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Uses and Disclosures of Protected Health Information

POLICY NUMBER: 016-79-09-02

Table of Contents:

1. PURPOSE

It is the policy of Yamhill County Health and Human Services (YCHHS) to protect the privacy of information about individuals to whom we provide services in accordance with all Federal and Oregon law. The intent of this policy is to specify that client or participant information cannot be used or disclosed without the individual's prior authorization, and to identify those exceptions that could be applicable.

2. TERMS

- ***Authorization (§164.508):*** Permission by an Individual, or a person's Personal Representative(s) for the release or use of information. An "authorization" is a written document that gives YCHHS permission to obtain and use information from third parties for specified purposes or to disclose information to a third party specified by the individual.
- ***Central Registry* (42 CFR Part 2, §2.11):** An organization which obtains from two or more member programs patient identifying information about individuals applying for withdrawal management or maintenance treatment for the purpose of avoiding an individual's concurrent enrollment in more than one treatment program.
- ***Consent (§164.506):*** YCHHS utilizes the *Consent to Treatment Form* in part to document individual's awareness that YCHHS uses and discloses health information for purposes of treatment, to obtain payment and to conduct health care operations.
- ***Disclosure* (§160.103)*:*** The release, transfer, provision of, access to, or divulging in any other manner of information outside an entity, such as YCHHS, holding such information.
- ***Lawful Holder (Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data, SAMHSA Fact Sheet):*** An individual or entity who has received patient identifying information as the result of a part 2-compliant consent or as otherwise permitted under the part 2 statute, regulations, or guidance.
- ***Member Program* (42 CFR Part 2, §2.11)**: A withdrawal management or maintenance treatment program which reports patient identifying information to a central registry and which is in the same state as that central registry or is in a state that participates in data sharing with the central registry of the program in question.
- ***Presumption of good faith belief (§164.512(j)(4):*** A covered entity that uses or discloses protected health information is…presumed to have acted in good faith with regard to a belief…if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.
- ***Psychotherapy Notes (§164.501)***: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and <u>that are separated from the rest of the individual's medical record</u>.

  Please note by HIPAA definition that:

  1. *Psychotherapy notes* are not the same as the YCHHS service note. They are very distinct, as noted above, and do not include such things as: medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the service plan, symptoms, prognosis, service notes, and progress to date; and
  2. *Psychotherapy notes* are personal notes recorded by the clinician, and by definition, not intended for others; and
  3. *Psychotherapy notes* should not be retained in the YCHHS electronic health record or the client's physical chart.

- ***Treatment, Payment and Operations (TPO (§164.501):***

- ➔ **Treatment:** The provision, coordination, or management of heath care and related services by one or more health care provider, including the coordination or management of health care by a health care provider with the third party; consultation between health care providers relating to a client or the referral of a client for health care from one health care provider to another.
- ➔ **Payment:** Any activities undertaken by YCHHS related to an individual to whom health care or payment for health care is provided in order to:
  - ❖ Obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan;
  - ❖ Obtain or provide reimbursement for the provision of health care.
- ➔ **Operations:** Any activities undertaken by YCHHS related to:
  - ❖ Conducting quality assessments, reviewing the competence and qualifications of staff;
  - ❖ Underwriting, premium rating and other activities related to health insurance or health benefits;
  - ❖ Conducting or arranging for medical reviews, legal services and auditing functions, including fraud and abuse detection and compliance programs;
  - ❖ Business planning and development and general administrative activities.

❖ ***Use* (§160.103):** The sharing, employment, application, utilization, examination, or analysis of protected health information within an entity, such as YCHHS, that maintains such information.

3. INDIVIDUAL CONSENT TO TREATMENT

A. **General Procedures:**

A.1. A signed YCHHS *Consent to Treatment Form* will be obtained to use an individual's health information for purposes of treatment, payment or health care operations except as otherwise described in this Policy.

A.2. **Behavioral Health Only:** In addition to the signed *Consent to Treatment*, an authorization, meeting all the required elements of an authorization (ROI), to a third-party payer is required per 42 CFR Part 2, §2.31.

B. **Exceptions to Signed Consent to Treatment Requirement:**

B.1. YCHHS is not required to obtain an individual's signed consent in the following situations:

B.1.1. **Indirect Treatment Relationship:** Where YCHHS is delivering health care to an individual based on the order/contract of another health care provider (i.e., the direct treatment provider), and YCHHS will deliver diagnosis or results directly to the ordering health care provider who will relay the results to the individual (i.e., jail contracts). (Not applicable for 42 CFR part 2).

B.1.2. **Emergency:** No consent is required when in an emergency treatment situation, as long as YCHHS attempts to obtain the individual's signature on the consent form as soon as reasonably practicable.

B.1.3. **As Required by Law:** No consent is required when YCHHS is required by law to treat the individual and YCHHS has attempted to obtain the consent but is unable to obtain such consent.

B.1.4. **Communication Barrier:** No consent is required when the individual is unable to sign the consent due to substantial barriers in communicating and staff can infer the individual's consent from the circumstances. (Not applicable for 42 CFR part 2).

a) Where consent is inferred, staff must document the attempt to obtain the signed consent form and document the reason that the consent form could not be signed. If the communication barrier is later removed, staff must obtain the signed consent at that time. (Not applicable for 42 CFR part 2).

C. **Refusal to Sign a Consent to Treatment:**

C.1. Except as stated in Subsection B.1.3 of this policy, if an individual refuses to sign the consent form, YCHHS may refuse to provide treatment to the individual. If staff provides treatment in spite of the individual's refusal, staff must document such refusal in the individual's medical record.

4. INDIVIDUAL AUTHORIZATION (§164.508 TO 512)

A. **General Procedures:**

A.1. YCHHS shall not use or disclose any information about a client or participant of YCHHS programs or services without a signed authorization for release of that information from the individual, or the individual's personal representative, unless authorized by this Policy, or as otherwise required by state or federal law.

A.2. Valid authorization at a minimum will include the following (§164.508(c):

A.2.1. Core Elements:

a) The name of the patient.

b) Description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

c) Name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

1) **Behavioral Health Only (42 CFR Part 2, §2.31)**: The specific name(s) or general designation(s) of the part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure.

d) Name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use of disclosure.

1) **Behavioral Health Only (42 CFR Part 2, §2.31)**:

i. The name(s) of the individual(s) or the name(s) of the entity(-ies) to which a disclosure is to be made.

ii. Special instructions for entities that facilitate the exchange of health information and research institutions. Notwithstanding paragraph (d)(1)(i) of this section, if the recipient entity facilitates the exchange of health

information or is a research institution, a written consent must include the name(s) of the entity(-ies) and

A.2.1.d.1.ii.1. The name(s) of individual or entity participant(s); or

A.2.1.d.1.ii.2. A general designation of an individual or entity participant(s) or class of participants that must be limited to a participant(s) who has a treating provider relationship with the patient whose information is being disclosed. When using a general designation, a statement must be included on the consent form that the patient (or other individual authorized to sign in lieu of the patient), confirms their understanding that, upon their request and consistent with this part, they must be provided a list of entities to which their information has been disclosed pursuant to the general designation (see §2.13(d)).

e) Description of each purpose of the requested use or disclosure.

f) Expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.

g) Signature of the individual and date signed. If signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

A.2.2. Required Statements:

a) Individual's right to revoke the authorization and description of how the individual may revoke the authorization.

b) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization; or consequences to the individual of a refusal to sign the authorization.

c) **Behavioral Health Only**: Prohibition on re-disclosure – each disclosure made with the individual's written authorization must be accompanied by the following statement:

"This record which has been disclosed to you is protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of this record unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or, is otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see§2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §2.12(c)(5) and 2.65" (42 CFR part 2, §2.32).

A.2.3. Written in plain language.

A.2.4. Provide the individual with a copy of the signed authorization.

B. **Public Health (§164.512(b):**

B.1. For the purpose of carrying out duties in its role as a public health authority, YCHHS does not need to obtain an individual's authorization to lawfully receive, use, disclose or exchange protected information (see Section 4. "Allowable Uses and Disclosures for Which an Authorization or Opportunity to Agree or Object is not Required" activities Policy #016-79-09-03, Public Health Uses and Disclosures of Protected Health Information).

C. **When an Authorization is required:**

C.1. Except as otherwise permitted or required by law and consistent with these policies, YCHHS shall obtain a completed and signed authorization for release of information from the individual, or the individual's personal representative, before obtaining or using information about an individual from a third party or disclosing any information about the individual to a third party.

D. **Re-disclosure of an Individual's Information:**

D.1. Unless prohibited by State and Federal laws, information held by YCHHS and authorized by the individual for disclosure may be subject to re-disclosure and no longer protected by YCHHS policy. Whether or not the information remains protected depends on whether the recipient is subject to Federal or State privacy laws, court protective orders or other lawful process.

D.2. Vocational Rehabilitation and Alcohol and Drug Rehabilitation information: Federal regulations (42 CFR part 2 and 34 CFR 361.38) prohibit HHS from making further disclosure of vocational rehabilitation and alcohol and drug rehabilitation information without the specific written authorization of the individual to whom it pertains.

D.3. **Behavioral Health Only:** 42 CFR Part 2 requires each disclosure made with the patient's written consent be accompanied by the statement found above at A.2.2(c) of this Section.

D.3.1. A non-part 2 treating provider that receives patient records from a part 2 provider and notified of the prohibition on re-disclosure may record information about a substance use disorder (SUD) and its treatment that identifies a patient. This is permitted and does not constitute a record that has been re-disclosed under part 2, provided that any SUD records received from a part 2 program or other lawful holder are segregated or segmented. The act of recording information about a SUD and its treatment does not by itself render a medical record which is created by a non-part 2 treating provider subject to the restrictions of this part 2. (§2.12(d)(2)(ii))

D.4. **Behavioral Health Only (42 CFR Part 2, §2.33(b):**

D.4.1. If a patient consents to a disclosure of their records under §2.31, a part 2 program may disclose those records in accordance with that consent to any person or category of persons identified or generally designated in the consent, except that disclosures to central registries and in connection with criminal justice referrals must meet the requirements of §§2.34 and 2.35, respectively.

D.4.2. If a patient consents to a disclosure of their records under §2.31 for payment or health care operations activities, a lawful holder who receives such records under the terms of the written consent may further disclose those records as may be necessary for its contractors, subcontractors, or legal representatives to carry out payment and/or health care operations on behalf of such lawful holder. In accordance with §2.13(a), disclosures under this section must be limited to that information which is necessary to carry out the stated purpose of the disclosure. Examples of permissible payment or health care operations activities under this section include:

a) Billing, claims management, collections activities, obtaining payment under a contract for reinsurance, claims filing, and/or related health care data processing;

b) Clinical professional support services (e.g., quality assessment and improvement initiatives; utilization review and management services);

c) Patient safety activities;

d) Activities pertaining to:

   1) The training of student trainees and health care professionals;

   2) The assessment of practitioner competencies;

   3) The assessment of provider or health plan performance; and/or

   4) Training of non-health care professionals;

e) Accreditation, certification, licensing, or credentialing activities;

f) Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and/or ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care;

g) Third-party liability coverage;

h) Activities related to addressing fraud, waste and/or abuse;

i) Conducting or arranging for medical review, legal services, and/or auditing functions;

j) Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating, including formulary development and administration, development or improvement of methods of payment or coverage policies;

k) Business management and general administrative activities, including management activities relating to implementation of and compliance with the requirements of this or other statutes or regulations;

l) Customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers;

m) Resolution of internal grievances;

n) The sale, transfer, merger, consolidation, or dissolution of an organization;

o) Determinations of eligibility or coverage (e.g., coordination of benefit services or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

p) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

q) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

r) Care coordination and/or case management services in support of payment or health care operations; and/or

s) Other payment/health care operations activities not expressly prohibited in this provision.

D.4.3. Lawful holders who wish to disclose patient identifying information pursuant to paragraph (4.2) of this section must have in place a written contract or comparable legal instrument with the contractor or voluntary legal representative, which provides that the contractor, subcontractor, or voluntary legal representative is fully bound by the provisions of part 2 upon receipt of the patient identifying information. In addition, YCHHS will also execute a Business Associate Agreement and/or Qualified Service Organization agreement with the contractor or voluntary legal representative.

D.5. Oregon law and administrative rule (ORS 433.045 and OAR 333-022-0210) prohibits further disclosure of HIV information.

D.6. Oregon law and administrative rule (ORS 192.531 to 192.549 and OAR 333-025-0100-0165) prohibits further disclosure of Genetics information without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations. A general authorization for the release of medical information is not sufficient for this purpose.

D.7. Oregon law (ORS 179.505) places restrictions on disclosure of information regarding clients of publicly funded mental health or developmental disability providers.

E. **Behavioral Health Only (42 CFR Part 2, §2.34, 36):** Disclosures to Central Registries and Prescription Drug Monitoring Program

E.1. Disclosures to Prevent Multiple Enrollments. (§2.34)

E.1.1. Restrictions on disclosure. A part 2 program, as defined in §2.11, may disclose patient records to a central registry or to any withdrawal management or maintenance treatment program not more than 200 miles away for the purpose of preventing the multiple enrollment of a patient only if:

a) The disclosure is made when:

1) The patient is accepted for treatment;

2) The type or dosage of the drug is changed; or

3) The treatment is interrupted, resumed or terminated.

b) The disclosure is limited to:

1) Patient identifying information;

2) Type and dosage of the drug; and

3) Relevant dates.

c) The disclosure is made with the patient's written consent meeting the requirements of §2.31, except that:

1) The consent must list the name and address of each central registry and each known withdrawal management or maintenance treatment program to which a disclosure will be made; and

2) The consent may authorize a disclosure to any withdrawal management or maintenance treatment program established within 200 miles of the program, but does not need to individually name all programs.

E.1.2. Use of information limited to prevention of multiple enrollments. A central registry and any withdrawal management or maintenance treatment program to which information is disclosed to prevent multiple enrollments may not re-disclose or use patient identifying information for any purpose other than the prevention of multiple enrollments or to ensure appropriate coordinated care with a treating provider that is not a part 2 program unless authorized by a court order under 42 CFR Part 2, Subpart E of this part.

E.1.3. Permitted disclosure by a central registry to prevent a multiple enrollment. When a member program asks a central registry if an identified patient is enrolled in another member program and the registry determines that the patient is so enrolled, the registry may disclose:

a) The name, address, and telephone number of the member program(s) in which the patient is already enrolled to the inquiring member program; and

b) The name, address, and telephone number of the inquiring member program to the member program(s) in which the patient is already enrolled. The member programs may communicate as necessary to verify that no error has been made and to prevent or eliminate any multiple enrollments.

E.1.4. Permitted disclosure by a central registry to a non-member treating provider, to prevent a multiple enrollment. When, for the purpose of preventing multiple program enrollments or duplicative prescriptions, or to inform prescriber decision making regarding prescribing of opioid medication(s) or other prescribed substances, a provider with a treating provider relationship that is not a member program asks a central registry if an identified patient is enrolled in a member program, the registry may disclose:

a) The name, address, and telephone number of the member program(s) in which the patient is enrolled;

b) Type and dosage of any medication for substance use disorder being administered or prescribed to the patient by the member program(s); and

c) Relevant dates of any such administration or prescription. The central registry and non-member program treating prescriber may communicate as necessary to verify that no error has been made and to prevent or eliminate any multiple enrollments or improper prescribing.

E.1.5. Permitted disclosure by a withdrawal management or maintenance treatment program to prevent a multiple enrollment. A withdrawal management or maintenance treatment program which has received a disclosure under this Section and has determined that the patient is already enrolled may communicate as necessary with the program making the disclosure to verify that no error has been made and to prevent or eliminate any multiple enrollments.

E.2. Disclosures to prescription drug monitoring programs. (§2.36)

E.2.1. A part 2 program or other lawful holder is permitted to report any SUD medication prescribed or dispensed by the part 2 program to the applicable state prescription drug monitoring program if required by applicable state law. A part 2 program or other lawful holder must obtain patient consent to a disclosure of records to a prescription drug monitoring program under §2.31 prior to reporting of such information.

F. **Revocation of Authorization (§164.508(b)(5):**

F.1. A client may revoke an authorization at any time. To revoke an authorization the client is encouraged to submit the revocation in writing that specifies the authorization to be revoked. A verbal revocation from the client will be accepted. YCHHS staff need to document this verbal revocation in the client's record. A revocation will be effective immediately unless the client specifies a future date in written revocation.

F.1.1. The revocation will not be valid where YCHHS has already taken action or used the authorization.

F.2. YCHHS' *Authorization for Use and Disclosure of Information* form shall include a statement that the individual can cancel or revoke the authorization at any time (§164.508(c) (2) and 42 CFR Part 2 §2.31(8).

G. **Conflicting Authorizations**:

G.1. Where the terms of an authorization conflicts with the terms of another authorization (or with the terms of another written communication from the individual) staff shall attempt to resolve the conflict. Staff shall communicate with the individual to determine current intent and by obtaining the individual's signature on a new authorization that reflects the individual's current intent.

H. **Verification of Individuals Requesting Information (§164.514(h)(1) and 5b.5(b)**:

H.1. Information about an individual may not be disclosed without verifying the identity of the person requesting the information, if the YCHHS staff member fulfilling the request does not know that person.

H.2. YCHHS staff will seek information to confirm the identity of the person requesting protected health information (PHI). The person requesting the information must provide reasonable evidence to verify their identity. Some examples include: an identification badge, driver's license, written statement of identity on agency letterhead, or similar proof. If the requestor is a Provider, have them give you their telephone number for a call back.

I. **Denial of Requests for Information:**

I.1. Unless an individual has signed an authorization, or the information about the individual can be disclosed pursuant to this Policy, YCHHS shall deny any request for individual information.

J. **When is an Authorization or opportunity to agree or object *NOT* required (§164.512 and 42 CFR Part 2 §2.12(c):**

J.1. HIPAA and 42 CFR Part 2:

J.1.1. Business Associate or Qualified Service Organization per agreement (§164.502).

J.1.2. Crimes on program premises or against program personnel, or threat to commit such a crime.

J.1.3. If YCHHS has reasonable cause to believe that a child is a victim of abuse or neglect, YCHHS may disclose protected information to appropriate governmental authorities authorized by law to receive reports of child abuse or neglect.

J.1.4. Internal Communication:

a) Internal communication within YCHHS is permitted without individual authorization, in compliance with Policy 016-79-09-06, *Minimum Necessary Information*.

1) Alcohol and drug, mental health, and vocational rehabilitation records' disclosure may be limited to particular program areas named on the authorization form. If such a limitation is noted on the authorization form, disclosure is limited to the parties named.

J.1.5. Medical emergencies (42 CFR part 2 §2.51 and §164.512(j): Patient identifying information may be disclosed to medical personnel to the extent necessary to:

a) Meet a bona fide medical emergency in which the patient's prior written consent cannot be obtained; or

b) Meet a bona fide medical emergency in which a part 2 program is closed and unable to provide services or obtain the prior written consent of the patient, during a temporary state of emergency declared by a state or federal authority as the result of a natural or major disaster, until such time that the part 2 program resumes operations.

c) Patient identifying information may be disclosed to medical personnel of the Food and Drug Administration (FDA) who assert a reason to believe that the health of any individual may be threatened by an error in the manufacture, labeling, or sale of a product under FDA jurisdiction, and that the information will be used for the exclusive purpose of notifying patients or their physicians of potential dangers.

d) Immediately following disclosure, the covered entity shall document the disclosure in the client's health record, including:

1) The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;

2) The name of the individual making the disclosure;

3) The date and time of the disclosure, and

4) The nature of the emergency (or error, if the report was to FDA).

J.1.6. Research activities (§164.512(i) and 42 CFR Part 2 §2.52):

a) YCHHS may disclose individual information without authorization for research purposes, as specified in Policy #016-79-09-04, *Uses and Disclosures for Research Purposes & Waivers*.

J.1.7. Audit and evaluation activities – HIPAA allows for Health Oversight Activities (see below). 42 CFR Part 2, §2.53 allows for audit and evaluation activities, but requires person reviewing records to agree in writing to comply with limitations on disclosure and use which states, "patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities as authorized by a court order entered under §2.66 of these regulations" (§2.53(d). See Policy 016-79-09-06(4)(C), *Minimum Necessary Information*, for additional information regarding audits and evaluations under 42 CFR Part 2, §2.53

J.2. **HIPAA Only:**

J.2.1. Where limited uses or disclosures are allowed WITHOUT an authorization or opportunity for individual to agree or object to the extent not prohibited or otherwise limited by federal or state requirements applicable to the program or activity.

J.2.2. Uses and Disclosures Required by Law:

a) YCHHS may use or disclose information without an individual's authorization if the law requires such use or disclosure, and the use or disclosure complies with, and is limited to, the relevant requirements of such law.

J.2.3. Adult Victims of Abuse, Neglect or Domestic Violence:

a) If YCHHS has reasonable cause to believe that an adult is a victim of abuse or neglect, YCHHS may disclose protected information, as required by law, to a government authority, including but not limited to social service or protective services agencies authorized by law to receive such reports.

b) YCHHS must inform the client that a report has been (or will be) made, unless:

1) YCHHS in the exercise of professional judgment, believes informing the client would place the client at risk of serious harm; or

2) YCHHS would be informing a personal representative, and YCHHS reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the client as determined by YCHHS in the exercise of professional judgment.

J.2.4. Health Oversight Activities:

a) YCHHS may disclose individual information without authorization for health oversight activities authorized by law, including audits; civil, criminal, or administrative investigations, prosecutions, or actions; licensing or

disciplinary actions; Medicaid fraud; or other activities necessary for oversight.

J.2.5. Judicial and Administrative Proceedings:

a) YCHHS may disclose Protected Health Information in the course of any judicial or administrative proceeding (so long as such disclosure is consistent with applicable federal and Oregon law, including laws regulating Highly Confidential Information and Oregon Rules of Civil Procedure, Rules 44 and 55 regarding production of records) in response to an order of a court, a subpoena, a discovery request or other lawful process.

J.2.6. Law Enforcement Officials:

a) For limited law enforcement purposes, to the extent authorized by applicable federal or state law, YCHHS may report certain injuries or wounds; provide information to identify or locate a suspect, victim, or witness; alert law enforcement of a death as a result of criminal conduct; and provide information which constitutes evidence of criminal conduct on YCHHS premises.

J.2.7. Decedents:

a) YCHHS may disclose to a coroner or medical examiner, for the purpose of identifying a deceased person, determining a cause of death, or other duties authorized by law. If YCHHS personnel are performing the duty or function of a coroner or medical examiner, they may use an individual's information for such purposes.

b) YCHHS may disclose individual information without authorization to funeral directors, consistent with applicable law, as needed to carry out their duties regarding the decedent. YCHHS may also disclose such information prior to, and in reasonable anticipation of, the death.

J.2.8. Organ and Tissue Procurement:

a) YCHHS may disclose individual information without authorization to organ procurement organizations or other entities engaged in procuring, banking, or transplantation of cadaver organs, eyes, or tissue, for the purpose of facilitating transplantation.

J.2.9. Health or Safety:

a) To avert a serious threat to health or safety, YCHHS may disclose individual information without authorization:

1) YCHHS believes in good faith that the information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

2) The report is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat (duty to warn);

3) See Policy #016-79-09-03, *Public Health Uses and Disclosures of Protected Health Information* and Policy #016-79-09-11, *Enforcement, Sanctions, and Penalties for Violations of Individual Privacy*, Section 4.

J.2.10. Specialized Government Functions:

a) YCHHS may disclose individual information without authorization for other specialized government functions, including authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities that federal law authorizes.

J.2.11. Correctional Institutions:

a) YCHHS may disclose limited information without authorization to a correctional institution or a law enforcement official having lawful custody of an inmate, for the purpose of providing health care or ensuring the health and safety of individuals or other inmates.

J.2.12. Psychotherapy notes:

a) YCHHS may use or disclose Psychotherapy notes (§164.508(a)(2):

1) Use by the originator of the psychotherapy notes for treatment;

2) In training programs where students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;

3) When a health oversight agency uses or discloses in connection with oversight of the originator of the psychotherapy notes; or

4) To the extent authorized under state law to defend YCHHS in a legal action or other proceeding brought by the individual;

5) If YCHHS in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public (§164.508(a)(2)(ii) and §164.512(j)(1)(i).

J.3. **Client or Participant's authorization that is NOT required if the person is informed in advance and is given a chance to object (§164.512):**

J.3.1. YCHHS informs the individual in advance and the person has been given an opportunity to object.

J.3.2. Unless otherwise protected by law, YCHHS may orally inform the individual and obtain and document the individual's oral agreement.

a) For individuals receiving alcohol and drug, mental health, or vocational rehabilitation services, oral permission is not sufficient and written authorization is required.

b) In case of an emergency, YCHHS may disclose individual information without authorization to the extent needed to provide emergency treatment.

J.4. **Behavioral Health Only: Orders authorizing the use of undercover agents and informants to investigate employees or agents of a part 2 program in connection with a criminal matter. (42 CFR Part 2, §2.67)**

J.4.1. Application. A court order authorizing the placement of an undercover agent or informant in a part 2 program as an employee or patient may be applied for by

any law enforcement or prosecutorial agency which has reason to believe that employees or agents of the part 2 program are engaged in criminal misconduct.

J.4.2. Notice. The part 2 program director must be given adequate notice of the application and an opportunity to appear and be heard (for the limited purpose of providing evidence on the statutory and regulatory criteria for the issuance of the court order in accordance with §2.67(c)), unless the application asserts that:

a) The part 2 program director is involved in the suspected criminal activities to be investigated by the undercover agent or informant; or

b) The part 2 program director will intentionally or unintentionally disclose the proposed placement of an undercover agent or informant to the employees or agents of the program who are suspected of criminal activities.

J.4.3. Criteria. An order under this section may be entered only if the court determines that good cause exists. To make this determination the court must find all of the following:

a) There is reason to believe that an employee or agent of the part 2 program is engaged in criminal activity;

b) Other ways of obtaining evidence of the suspected criminal activity are not available or would not be effective; and

c) The public interest and need for the placement of an undercover agent or informant in the part 2 program outweigh the potential injury to patients of the part 2 program, physician-patient relationships and the treatment services.

J.4.4. Content of order. An order authorizing the placement of an undercover agent or informant in a part 2 program must:

a) Specifically authorize the placement of an undercover agent or an informant;

b) Limit the total period of the placement to twelve months, starting on the date that the undercover agent or informant is placed on site within the program. The placement of an undercover agent or informant must end after 12 months, unless a new court order is issued to extend the period of placement;

c) Prohibit the undercover agent or informant from disclosing any patient identifying information obtained from the placement except as necessary to investigate or prosecute employees or agents of the part 2 program in connection with the suspected criminal activity; and

d) Include any other measures which are appropriate to limit any potential disruption of the part 2 program by the placement and any potential for a real or apparent breach of patient confidentiality; for example, sealing from public scrutiny the record of any proceeding for which disclosure of a patient's record has been ordered.

J.4.5. Limitation on use of information. No information obtained by an undercover agent or informant placed in a part 2 program under this section may be used to investigate or prosecute any patient in connection with a criminal matter or as the basis for an application for an order under §2.65.

5. FORMS

- YCHHS Form: “Authorization for Use and Disclosure of Information”
- YCHHS Form # 1021: “Disclosures Log/Release of Protected Health Information Tracking Log”
- YCHHS Form # 1022: “Access to Records and Accounting of Disclosures Request”

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Public Health Uses and Disclosures of Protected Health Information

POLICY NUMBER: 016-79-09-03

Table of Contents:

1. PURPOSE

It is the policy of Yamhill County Health and Human Services (YCHHS) to protect the privacy of information about individuals to whom we provide services in accordance with all federal and Oregon law. This policy does not prohibit YCHHS from receiving, using, or disclosing an individual's protected information in its role as a governmental public health authority; nor does it prohibit disclosure of such information to other governmental public health authorities.

2. TERMS

- ***Authorization (§164.508)****:* Permission by an Individual, or individual's Personal Representative(s) for the release or use of information. An "authorization" is a written document that gives YCHHS permission to obtain and use information from third parties for specified purposes or to disclose information to a third party specified by the individual.
- ***Consent (§164.506)****:* YCHHS utilizes the *Consent to Treatment Form* in part to document individual's awareness that YCHHS uses and discloses health information for purposes of treatment, to obtain payment and to conduct health care operations.

- ***Disclosure* (§160.103)*:*** The release, transfer, or divulging of information outside an entity, such as YCHHS, holding such information.
- ***Treatment, Payment and Operations (TPO) (§164.501):***
  - ➔ **Treatment:** The provision, coordination, or management of health care and related services by one or more health care provider, including the coordination or management of health care by a health care provider with the third party; consulting between health care providers relating to a patient or the referral of a patient for health care from one health care provider to another.
  - ➔ **Payment:** Any activities undertaken by YCHHS related to an individual to whom health care or payment for health care is provided in order to:
    - Obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan;
    - Obtain or provide reimbursement for the provision of health care.
  - ➔ **Operations:** Any activities undertaken by YCHHS related to:
    - Conducting quality assessments, reviewing the competence and qualifications of staff;
    - Underwriting, premium rating and other activities related to health insurance or health benefits or medical reviews;
    - Business planning, development, and general administrative activities.
- ***Use* (§160.103)*:*** The sharing, employment, application, utilization, examination, or analysis of protected health information within an entity, such as YCHHS, that maintains such information.

3. USES AND DISCLOSURES

A. General Procedures:

A.1. Information about individuals received or held by YCHHS as a governmental public health authority shall be safeguarded against loss, interception or misuse.

A.2. YCHHS does not need to obtain an individual's authorization to lawfully receive, use, or disclose an individual's protected information in its role as a governmental public health authority; nor does YCHHS need authorization with respect to exchanges of such information with other governmental public health authorities, or as otherwise required or permitted by law (§164.512(b).

4. ALLOWABLE USES AND DISCLOSURES FOR WHICH AN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT IS NOT REQUIRED (§164.512(B)

A. Disclosures for Public Health Activities:

A.1. YCHHS may disclose an individual's protected information for governmental public health activities and purposes to:

A.1.1. A governmental public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. This includes but is not limited to reporting disease, injury,

vital events such as birth or death, and the conducting of public health surveillance, investigations, and interventions;

A.1.2. An official of a foreign government agency that is acting in collaboration with a lawful governmental public health authority;

A.1.3. A governmental public health authority, or other appropriate government authority, that is authorized by law to receive reports of child abuse or neglect;

A.1.4. A person subject to the jurisdiction of the federal Food and Drug Administration (FDA), regarding an FDA-regulated product or activity for which that person is responsible, for activities related to the quality, safety, or effectiveness of such FDA-related product or activity. Such purposes include:

a) To collect or report adverse events, product defects or problems (including product labeling problems), or biological product deviations;

b) To track FDA-related products;

c) To enable product recalls, repairs, or replacement, or look back; or

d) To conduct post market surveillance.

A.1.5. A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition. If YCHHS, or other public health authority, is authorized by law to notify such person as necessary in conducting a public health intervention or investigation.

A.1.6. An employer, about an individual who is a member of the workforce of the employer, if the conditions in §164.512(b)(v) are met.

A.1.7. A school, about an individual who is a student or prospective student of the school, if the conditions of §164.512(b)(vi) are met.

A.1.8. As a public health authority, YCHHS is authorized to use and disclose an individual's protected information in all cases in which YCHHS is permitted to disclose such information for the public health activities listed above.

A.1.9. Public health research will be conducted consistent with YCHHS Policy #016-79-09-04**,** *Uses and Disclosures for Research Purposes & Waivers*.

A.1.10 Where State or Federal law prohibits or restricts uses and disclosure of information obtained or maintained for public health purposes, such use and disclosure shall be denied or restricted.

B. **Operation of the Public Health Laboratory:**

B.1. State law establishes that for the "protection of the public health", a Public Health Laboratory is created within YCHHS to conduct tests and examinations at the request of any state, county, or city institution or officer, and at the request of any licensed physician.

B.2. Laboratories are health care providers with an "indirect treatment relationship" as defined in federal regulations 45 CFR 164.501 and in accordance with 45 CFR 164.506.

B.3. YCHHS is authorized to use and disclose information for purposes of the operation of the Public Health Laboratory consistent with HIPAA and applicable law.

C. **Verifying the authority of a public health officer:**

C.1. Health care providers and health care payers may request YCHHS to verify the authority of a YCHHS employee or contractor to conduct a public health activity. YCHHS employees or contractors must be prepared to explain and provide documentation, to the provider or payer, their legal authority to collect or obtain information and be prepared to identify (§164.514(h).

5. EXCEPTIONS ALLOWING LIMITED DISCLOSURES WITHOUT AUTHORIZATIONS (§164.512)

To the extent not otherwise prohibited or limited by federal or state requirements applicable to the YCHHS program or activity, YCHHS may use or disclose protected information without the written authorization of the individual in the following circumstances:

A. Individuals who requested disclosure to themselves.

B. YCHHS may disclose information without authorization for its own treatment, payment or health care operations.

C. YCHHS may disclose information without authorization to another covered entity or a health care provider for the payment activities or the entity that receives the information (§164.506(c).

D. YCHHS may disclose information without authorization to another entity covered by federal HIPAA law and rules for the health care activities of that entity, if:

D.1. Both that entity and YCHHS has or has had a relationship with the individual who is the subject of the information;

D.2. The information pertains to such relationship; and

D.3. The disclosure is for the purpose of (§164.501 – *Health care operations)*:

D.3.1. Conducting quality assessment and improvement activities, including: outcome evaluation and development of clinical guidelines, provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or

D.3.2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing, or credentialing activities; or

D.3.3. Detecting health care fraud and abuse or for compliance purposes (§164.506(c).

E. YCHHS may use or disclose information without the written authorization of the individual if YCHHS has reasonable cause to believe that child is a victim of abuse or neglect, YCHHS may disclose information to appropriate governmental authorities authorized by law to receive reports of child abuse or neglect.

F. YCHHS may use or disclose information without the written authorization of the individual if YCHHS has reasonable cause to believe that an **adult** is a victim of abuse or neglect (elder abuse, nursing home abuse, or abuse of the mentally ill or developmentally disabled). YCHHS may disclose protected information to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse or neglect: (§164.512(c).

F.1. If the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law; or

F.2. If the individual agrees to the disclosure, either orally or in writing; or

F.3. To the extent the disclosure is expressly authorized by statute or regulation and:

F.3.1. When YCHHS staff, in the exercise of professional judgment and in consultation with appropriate YCHHS supervisor, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

F.3.2. When the individual is unable to agree because of incapacity, a law enforcement agency or other public official authorized to receive the report represents that:

a) The protected information being sought is not intended to be used against the individual, and

b) An immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

F.4. When YCHHS staff make a disclosure permitted above, YCHHS must promptly inform the individual that such a report has been or will be made, except if:

F.4.1. YCHHS staff, in the exercise of professional judgment and in consultation with appropriate YCHHS supervisor, believes informing the individual would place the individual or another individual at risk of serious harm; or

F.4.2. YCHHS staff would be informing a personal representative and YCHHS staff reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing such person would not be in the best interests of the individual, as determined by YCHHS staff, in the exercise of professional judgment and in consultation with appropriate YCHHS supervisor.

G. YCHHS may use or disclose information without the written authorization of the individual for the purpose of carrying out duties in its role as a health oversight agency, YCHHS does not need to obtain an individual's authorization to lawfully receive, use or disclose individual information for oversight activities authorized by law.

G.1. YCHHS may disclose information to a health oversight agency to the extent the disclosure is not prohibited by state or federal law for its oversight activities of:

G.1.1. The health care system;

G.1.2. Government benefit programs for which the information is relevant to eligibility;

G.1.3. Entities subject to government regulatory programs for which the information is necessary for determining compliance with program standards; or

G.1.4. Entities subject to civil rights laws for which the information is necessary for determining compliance.

G.2. **Exception**: a health oversight activity for which information may be disclosed does ***not*** include an investigation or other activity of which the individual is the subject ***unless*** the investigation or other activity is directly related to:

G.2.1. The receipt of health care;

G.2.2. A claim to recover public benefits related to health; or

G.2.3. Qualifying for or receiving public benefits or services based on the health of the individual.

G.3. If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity is considered a health oversight activity for purposes of this Section.

G.4. When YCHHS is acting as a health oversight agency, YCHHS may use information for health oversight activities as permitted under this section.

H. YCHHS may use or disclose information without the written authorization for the individual when YCHHS disclose information in a judicial or administrative proceeding subject to the following (§164.512(e).

H.1. YCHHS must follow any procedures for responding to subpoenas, discovery requests, or other requests for documents that YCHHS may have regarding an individual; YCHHS must not ignore any subpoena or other legal document. See YCHHS Policy #016-79-04-13, *Subpoenas*.

H.1.1. In general, YCHHS will respond by appearing before the Court to explain that the information is confidential, or by filing a legal response through the Department of Justice. YCHHS will not disclose any confidential information in a court proceeding in which YCHHS is not a party except as required by law or by a court order.

H.1.2. An administrative hearings officer or administrative law judge lacks legal authority, under Oregon law, to require or authorize YCHHS to disclose information about an individual that is confidential under federal or state law. YCHHS staff should work with hearing officers to ensure that protective orders are used when appropriate in contested case hearings to prevent authorized uses and disclosures of information.

H.1.3. YCHHS staff will refer any questions or concerns regarding what is required by law, or by a court order, to the YCHHS Privacy Officer, who may then consult with the Department of Justice to resolve the question.

H.1.4. **Exception:** YCHHS may disclose information regarding mental health, alcohol or drug treatment, and vocational rehabilitation services only if required by a court order (ORS 179.505). For civil commitment proceedings, previous mental health histories may not be released.

H.2. YCHHS may use or request information to investigate a grievance or appeal made to YCHHS about an individual's eligibility or right to benefits or services.

H.2.1. Pursuant to applicable laws and rules, YCHHS may use or disclose information that YCHHS has compiled on its own or has received from external sources.

H.2.2. That information may be reviewed by YCHHS staff and legal counsel, the providers or health plan involved in the service or action, and may be provided to a hearing officer, to assist YCHHS in making a decision about the appeal or grievance.

H.3. If YCHHS is sued or if a suit is filed on behalf of YCHHS, the Department of Justice will address or respond to legal issues related to the use and disclosure of information. YCHHS will identify confidentiality issues for discussion with the assigned legal counsel, in consultation with the YCHHS Privacy Officer.

H.4. If a court orders YCHHS to conduct a mental examination (such as in accordance with state law at ORS 161.315, 161.365, 161.370, ORS 419B.352), or orders YCHHS to provide any other report or evaluation to the court such examination, report or evaluation shall be deemed to be "required by law" for purposes of HIPAA, and YCHHS staff will comply with the court order.

H.5. If YCHHS has obtained information in performing its duties as a health oversight agency, public health authority, protective service entity, or public benefit program, nothing in this section supersedes YCHHS policies that otherwise permit or restrict uses or disclosures. For example, if YCHHS has obtained individual patient information as a result of an oversight action against a provider, YCHHS may lawfully use that patient information in a hearing consistent with the other confidentiality requirements applicable to that program, service or activity.

H.6. In any case, in which federal or state law prohibits or restricts the use or disclosure of information in an administrative or judicial proceeding, YCHHS shall assert the confidentiality of such confidential information, consistent with YCHHS policies applicable to the program, service or activity, to the presiding officer at the proceeding. A HIPAA-authorized protective order may not be sufficient to authorize disclosure if it does not address other applicable confidentiality laws.

I. YCHHS may use or disclose information without the written authorization of the individual for law enforcement purposes unless federal or state law prohibits such disclosure.

I.1. YCHHS may disclose information when reporting certain types of wounds or other physical injuries.

I.2. YCHHS may disclose information in compliance with, and limited to the relevant specific requirements of:

I.2.1. A court order or warrant, summons or subpoena issued by a judicial officer;

I.2.2. A grand jury subpoena; or

I.2.3. An administrative request, including administrative subpoena or summons, a civil or authorized investigative demand, or similar lawful process, provided that:

a) The information is relevant, material, and limited to a legitimate law enforcement inquiry;

b) The request is specific and limited in scope to the extent reasonably practical in light of the purpose for which the information is sought; and

c) De-identified information could not reasonably be used.

d) **Exception:** Information regarding mental health, alcohol or drug treatment, and vocational rehabilitation services can be disclosed only based on a court order (ORS 179.505, 42CFR Part 2).

I.3. YCHHS may disclose limited protected information upon request of a law enforcement official without authorization for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that (§164.512f):

I.3.1. The information YCHHS may thus disclose is limited to:

a) Name and address;

b) Date and place of birth;

c) Social security number;

d) ABO blood type and rh factor;

e) Type of injury;

f) Date and time of treatment;

g) Date and time of death if applicable; and

h) A description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of beard or mustache, scars, and tattoos. In cases of criminal court commitments, a photograph may be provided.

Exceptions:

i) **Behavioral Health Only:** 42 CFR Part 2 does not allow disclosure of client alcohol and drug information to law enforcement except in response to crimes on program premises or against program personnel, or threat to commit such a crime; reports of suspected child abuse; and neglect or in response to court order(§2.12 and §2.61(b).

❖ YCHHS may not disclose, for purposes of identification or location, protected health information related to the subject's DNA or DNA analysis, dental records, or typing, samples, or analysis of bodily fluids or tissues, unless ordered to do so by a court or a court approved search warrant.

I.4. YCHHS may disclose protected information upon request to a law enforcement official about an individual who is or is suspected to be the victim of a crime, if:

I.4.1. YCHHS is otherwise authorized by law to disclose that information for purposes of an abuse reporting law or for public health or heath oversight purposes; or

I.4.2. The individual agrees to the disclosure, either orally or in writing;

I.4.3. YCHHS is unable to obtain the individual's agreement due to incapacity or emergency circumstance, if:

a) The law enforcement official represents that such information is needed to determine whether a violation of law by someone other than the victim has occurred and such information is not intended for use against the victim;

b) The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

c) YCHHS determines that the disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

I.5. YCHHS may disclose protected information to a law enforcement official about an individual who has died, for the purpose of alerting law enforcement of the death, if YCHHS suspects that death may have resulted from criminal conduct.

I.6. YCHHS may disclose protected information to a law enforcement official if YCHHS believes in good faith that the information constitutes evidence of criminal conduct on YCHHS premises.

I.7. YCHHS may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if YCHHS, in good faith, believes the use or disclosure:

I.7.1. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

I.7.2. Is to a person or persons reasonably able to prevent or lessen the threat; or

I.7.3. Necessary for law enforcement authorities to identify or apprehend an individual:

a) Because of a statement by a person admitting participation in a violent crime that YCHHS reasonably believes may have caused serious harm to the victim; or

b) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

I.7.4. ***Exception***: Use or disclosure may not be made if the information is learned by YCHHS (§164.512(j)(2):

a) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or

b) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

J. YCHHS may disclose an individual's information without authorization for the following specialized government functions without individual authorization unless federal or state law prohibits such disclosure.

J.1. For individuals who are Armed Forces personnel, as deemed necessary by appropriate military command authorities to ensure the proper execution of the military mission.

J.2. To authorized federal officials for conducting lawful intelligence, counterintelligence, and other national security activities, as authorized by the federal National Security Act (50 U.S.C 401, et seq.) and implementing authority.

J.3. To authorized federal officials for the protection of the President or of other persons authorized by applicable federal law.

K. YCHHS may use or disclose information without the written authorization of the individual consistent with applicable law to a correctional institution or a law enforcement official having lawful custody of an inmate or other person, if the institution or official represents that the information is necessary for:

K.1. Providing health care to the person;

K.2. The health or safety of the person or of other inmates; or the officers or employees of, or others, at the correctional institution.

L. YCHHS may use or disclose protected information without the written authorization of the individual in the case of an emergency.

L.1. Medical emergencies (42 CFR part 2 §2.51 and §164.512(j).

L.1.1. Client information may be disclosed to medical personnel who have a need for information about a patient for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention.

L.1.2. Immediately following disclosure, the covered entity shall document the following disclosure in the client's health record:

a) The name of the medical personnel to whom disclosure was made and their affiliation with any health care facility;

b) The name of the individual making the disclosure;

c) The date and time of the disclosure, and

d) The nature of the emergency

L.2. Any disclosure of Protected Health Information must be recorded in the," YCHHS Form #1021: "Disclosures Log/Release of Protected Health Information Tracking Log" as outlined in YCHHS Policy # 016-79-09-01, *Client Rights*.

6. CLIENT OR PARTICIPANT AUTHORIZATION IS NOT REQUIRED IF THEY ARE INFORMED IN ADVANCE AND GIVEN A CHANCE TO OBJECT (§164.510)

A. In some limited circumstances, YCHHS may use or disclose an individual's information without authorization, but only if the individual has been informed in advance and has been given the opportunity to either agree or to object or restrict the use or disclosure. These circumstances are:

A.1. For disclosure of health care information to a family member, other relative, or close personal friend of the individual, or any other person named by the individual, subject to the following limitations.

A.1.1. YCHHS may reveal only the protected information that directly relates to such person's involvement with the individual's care or payment for such care.

A.1.2. YCHHS may use or disclose protected information for notifying (including identifying or locating) a family member, personal representative, or other

person responsible for care of the individual, regarding the individual's location, general condition, or death.

A.1.3. If the individual is present for, or available prior to, such a use or disclosure, YCHHS may disclose the protected information if it:

a) Obtains the individual's agreement;

b) Provides the individual an opportunity to object to the disclosure, and the individual does not express an objection; or

c) Reasonably infers from the circumstances that the individual does not object to the disclosure.

A.1.4. If the individual is not present, or the opportunity to object to the use or disclosure cannot practicably be provided due to the individual's incapacity or an emergency situation, YCHHS may determine, using professional judgment, that the use or disclosure is in the individual's best interests.

a) Any agreement, objection, refusal, or restriction by the individual, may be oral or in writing. YCHHS will document any such oral communication in the client's case file.

b) YCHHS will also document in the case file the outcome of any opportunity provided to object; the individual's decision not to object; or the inability of the individual to object.

NOTE: ***Oral permission to use or disclose information for purposes described in subsection (A) of this section is not sufficient when the individual is referred to or receiving substance use disorder treatment, mental health, or vocational rehabilitation services. Written authorization is required under those circumstances.***

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Uses and Disclosures for Research Purposes and Waivers

POLICY NUMBER: 016-79-09-04

Table of Contents:

1. PURPOSE

The intent of this policy is to specify when YCHHS may use or disclose information about individuals for research purposes.

2. TERMS

- *Common Rule:* is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human Services, and adopted by other federal governmental agencies, including the National Institutes for Health, for research funded by those agencies.
- *Research:* A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

3. GENERAL PROCEDURES

A. **When using or disclosing PHI for research purposes:**

A.1. YCHHS may use or disclose an individual's information for research purposes as specified in this policy.

A.2. All such research disclosures are subject to **applicable requirements** of state and federal laws and regulations and to the specific requirements of this policy.

A.3. **Note:**

A.3.1. This policy is intended to supplement existing research requirements of the Common Rule, 45 CFR Part 46. The Common Rule is the rule for the protection of human subjects in research promulgated by the U.S. Department of Health and Human Services, and adopted by other federal governmental agencies, including the National Institutes for Health, for research funded by those agencies. In addition, some agencies have requirements that supplement the Common Rule that are applicable to a particular research contract or grant.

A.3.2. **Behavioral Health Only:** See Section 5 (H) below for requirements under 42 CFR Part 2, §2.52.

B. **PHI cannot be used or disclosed for research purposes unless:**

B.1. An authorization for use or disclosure is obtained from the client; or

B.2. A waiver of authorization has been approved by an Institution Review Board (IRB); or

B.3. The health information has been de-identified, for purposes of research, consistent with YCHHS Policy # 016-79-09-05, *De-identification of Client Information and Use of Limited Data Sets*; or

B.4. The health information is used or disclosed in a Limited Data Set for purposes of research, consistent with the policies related to Limited Data Sets in YCHHS Policy # 016-79-09-05, *De-identification of Client Information and Use of Limited Data Sets*.

4. INSTITUTIONAL REVIEW BOARD (IRB) OR PRIVACY BOARD ESTABLISHED BY YCHHS

A. YCHHS may use an IRB established in accordance with 45 CFR Part 46 or a Privacy Board that has been established by YCHHS pursuant to this policy, to perform the duties and functions specified in this policy regarding a research project being conducted, in whole or in part, by YCHHS or by a YCHHS office or program.

5. USES AND DISCLOSURES FOR RESEARCH PURPOSES – SPECIFIC REQUIREMENTS

A. **Authorization:**

A.1. YCHHS must use or disclose client or participant information for research purposes with the client's specific written authorization unless an IRB waiver is obtained or information is de-identified.

A.1.1. Such authorization must meet all the requirements described in YCHHS Policy # 016-79-09-03, *Uses and Disclosures of Protected Health Information*, and may indicate as an expiration date such terms as "end of research study," or similar language.

A.1.2. An authorization for use and disclosure for a research study may be combined with any other type of written permission for the same research study. **For example:** The authorization may be in the same document as the consent to participate in research (§164.508(b)(3)(i).

A.1.3. If research includes treatment, the researcher may condition the provision of research related treatment on the provision of an authorization for use and disclosure of protected health information for such research (§164.508(b)(4)(i).

B. **When a Waiver of Authorization can be used:**

B.1. YCHHS may use or disclose client or participant information for research purposes without the client's or participant's written authorization provided that (§164.512(i)(1)(i):

a) YCHHS obtains documentation that a waiver of an individual's authorization for release of information requirements has been approved by either an Institutional Review Board (IRB) or Privacy Board that:

1) Has members with varying backgrounds and appropriate professional competency as needed to review the effect of the research protocol on the Individual's privacy rights and related concerns;

2) Includes at least one member who is not affiliated with YCHHS, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entity; and

3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

C. **Documentation Required of IRB or Privacy Board (§164.512(i)(2):**

C.1. When granting approval of a waiver, an individual's authorization for release of information must include:

C.1.1. A statement identifying the IRB or privacy board that approved the waiver of an individual's authorization, and the date of such approval;

C.1.2. A statement that the IRB or privacy board has determined that the waiver of authorization, in whole or in part, satisfies the following criteria:

a) The use or disclosure of an individual's protected information involves no more than minimal risk to the privacy of individuals, based on at least the following elements:

1) An adequate plan to protect an individual's identifying information from improper use or disclosure;

2) An adequate plan to destroy an individual's identifying information at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of the protected information would be permitted under this policy;

b) The research could not practicably be conducted without the waiver; and

c) The research could not practicably be conducted without access to, and use of, the Individual's protected information;

C.1.3. A brief description of the protected health information for which use or disclosure has been determined to be necessary by the IRB or privacy board;

C.1.4. A statement that the waiver of an individual's authorization has been reviewed and approved under either normal or expedited review procedures, by either an IRB or a privacy board, pursuant to federal regulations at 45 CFR 164.512(2); and

C.1.5. The Privacy Board Chair must sign documentation of the waiver of an individual's authorization, or other member as designated by the Chair of the IRB or the Privacy Board, as applicable.

D. **Requesting Access to individual information maintained by YCHHS:**

D.1. In some cases, a researcher may request access to individual information maintained by YCHHS in preparation for research or to facilitate the development of a research protocol in anticipation of research. Before agreeing to provide such access to individual information, YCHHS should determine whether federal or state law otherwise permits such use or disclosure without individual authorization or use of an IRB. If there is any doubt whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, YCHHS will only provide such access if YCHHS obtains, from the researcher, written representations that:

D.1.1. Use or disclosure is sought solely to review an individual's protected information needed to prepare a research protocol or for similar purposes to prepare for the research project;

D.1.2. No client information will be removed from YCHHS by the researcher in the course of the review;

D.1.3. The client information for which use or access is sought is necessary for the research purposes (§164.512(1)(ii);

D.1.4. Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than is provided for by the written agreement;

D.1.5. Researcher and his or her agents agree not to publicly identify the information or contact the individual whose data is being disclosed and (§164.514(e)(4)(C);

D.1.6. Applicable federal or state law may require such other terms or conditions.

E. **Requesting access of deceased client's individual information (164.512(1)(iii):**

E.1. In some cases, a researcher may request access to individual information maintained by YCHHS about individuals who are deceased. YCHHS should determine whether federal or state law otherwise permits such use or disclosure of information about decedents without individual authorization or use of an IRB. There may be instances where it would be inappropriate to disclose information, even where the individual subject of the

information is dead – for example, individuals who died of AIDS may not have wanted such information to be disclosed after their deaths. If there is any doubt whether the use and disclosure of the information by the researcher falls within this HIPAA exception, review by an IRB or privacy board and formal waiver of authorization is required. If such access falls within this HIPAA exception to authorization and is otherwise permitted by other federal or state law, YCHHS will only provide such access if YCHHS obtains the following written representations from the researcher:

E.1.1. Representation that the use or disclosure is sought solely for research on the protected information of deceased persons;

E.1.2. Documentation, if YCHHS so requests, of the death of such persons; and

E.1.3. Representation that the Individual's protected information for which use or disclosure is sought is necessary for the research purposes.

E.1.4. Researcher and his or her agents agree not to use or further disclose the information other than as provided in the written agreement, and to use appropriate safeguards to prevent the use or disclosure of the information other than what is provided for by the written agreement;

E.1.5. Researcher and his or her agents agree not to publicly identify the information or contact the personal representative or family members of the decedent; and

E.1.6. Applicable federal or state law may require such other terms or conditions.

F. **YCHHS Public Health Studies and Studies Required by Law (§164.512(b):**

F.1. When YCHHS is operating as a Public Health Authority, YCHHS is authorized to obtain and use individual information without authorization for the purpose of:

F.1.1. Preventing injury;

F.1.2. Preventing or controlling disease; and

F.1.3. Conducting of public health surveillance, investigations and interventions.

F.2. In addition to these responsibilities, YCHHS may collect, use or disclose information, without individual authorization, to the extent that such collection, use or disclosure is required by law.

F.2.1. When YCHHS uses information to conduct studies that are required by law, no additional individual authorization is required nor does this policy require IRB or privacy board waiver of authorization based on the HIPAA Privacy rules. Other applicable laws and protocols continue to apply to such studies.

G. **YCHHS Studies Related to Health Care Operations (§164.501):**

G.1. Studies and data analyses conducted for YCHHS's own quality assurance purposes and to comply with reporting requirements applicable to federal or state funding requirements fall within the uses and disclosures that may be made without individual authorization as YCHHS health care operations.

G.2. Neither individual authorization nor IRB or privacy board waiver of authorization is required for studies or data analyses conducted by or on behalf of YCHHS for purposes of health care operations, including any studies or analyses conducted to comply with

reporting requirements applicable to federal or state funding requirements. "Health care operations" as defined in 45 CFR 164.512 include:

G.2.1. Conducting *quality assessment and improvement activities*, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;

G.2.2. Conducting *population-based activities* relating to improving health care or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

G.2.3. Reviewing the *competence or qualifications* of health care professionals, evaluating practitioner and provider performance, health plan performance, and conducting training programs, and accreditation, certification, licensing or credentialing activities;

G.2.4. Underwriting, premium rating, and other activities related to the creation, renewal or replacement of a contract of *health insurance or health benefits*;

G.2.5. Conducting or arranging for *medical review, legal services, and auditing functions*, including fraud and abuse detection and compliance programs;

G.2.6. *Business planning and development*, such as conducting cost-management and planning related analyses related to managing and operating YCHHS, including improvement of administration or development or improvement of methods of payment or coverage policies; and

G.2.7. *Business management and general administrative activities* of YCHHS, including management activities related to HIPAA implementation and compliance; customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers; resolution of internal grievances; and

G.2.8. *Creating de-identified information* or a limited data set consistent with the YCHHS policy #016-79-09-05, *De-identification of Client Information and Use of Limited Data Sets*.

a) **Exception:** HIV-AIDS information may not be disclosed to anyone without the specific written authorization of the individual. Re-disclosure of HIV test information is prohibited, except in compliance with law or with written permission from the individual.

H. **Behavioral Health Only:** Research related to substance use disorder treatment follow restrictions and requirements of 42 CFR Part 2 §2.52.

H.1. Patient identifying information may be disclosed for the purpose of the recipient conducting scientific research if:

H.1.1. The program director makes a determination that the recipient of the client identifying information:

a) A HIPAA-covered entity or business associate that has obtained and documented authorization from the patient, or a waiver or alteration of authorization, consistent with the HIPAA Privacy Rule at 45 CFR 164.508 or 164.512(i), as applicable;

b) Subject to the HHS regulations regarding the protection of human subjects (45 CFR part 46), and provides documentation either that the researcher is in compliance with the requirements of 45 CFR part 46, including the requirements related to informed consent or a waiver of consent (45 CFR 46.111 and 46.116) or that the research qualifies for exemption under the HHS regulations (45 CFR 46.104) or any successor regulations;

c) Subject to the FDA regulations regarding the protection of human subjects (21 CFR parts 50 and 56) and provides documentation that the research is in compliance with the requirements of the FDA regulations, including the requirements related to informed consent or an exception to, or waiver of, consent (21 CFR part 50) and any successor regulations; or

d) Any combination of a HIPAA covered entity or business associate, and/or subject to the HHS regulations regarding the protection of human subjects, and/or subject to the FDA regulations regarding the protection of human subjects; and has met the requirements of paragraph (H.1)(H.1.1)(a), (b) (c), and/or (d) of this section, as applicable.

H.1.2. The part 2 program or other lawful holder of part 2 data is a HIPAA covered entity or business associate, and the disclosure is made in accordance with the HIPAA Privacy Rule requirements at 45 CFR 164.512(i).

H.1.3. If neither paragraph (H.1)(H.1.1) or (H.1.2) of this section apply to the receiving or disclosing party, this section does not apply.

H.2. Any individual or entity conducting scientific research using patient identifying information obtained under paragraph (H.1) of this section:

H.2.1. Is fully bound by the regulations in this part and, if necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by the regulations in this part.

H.2.2. Must not re-disclose patient identifying information except back to the individual or entity from whom that patient identifying information was obtained or as permitted under paragraph (H.3) of this section.

H.2.3. May include part 2 data in research reports only in aggregate form in which patient identifying information has been rendered non-identifiable such that the information cannot be re-identified and serve as an unauthorized means to identify a patient, directly or indirectly, as having or having had a substance use disorder.

H.2.4. Must maintain and destroy patient identifying information in accordance with the security policies and procedures established under §2.16.

H.2.5. Must retain records in compliance with applicable federal, state, and local record retention laws.

H.3. *Data linkages* –

H.3.1. Researchers. Any individual or entity conducting scientific research using patient identifying information obtained under paragraph (H.1) of this section that requests linkages to data sets from a data repository(-ies) holding patient identifying information must:

a) Have the request reviewed and approved by an Institutional Review Board (IRB) registered with the Department of Health and Human Services, Office for Human Research Protections in accordance with 45 CFR part 46 to ensure that patient privacy is considered and the need for identifiable data is justified. Upon request, the researcher may be required to provide evidence of the IRB approval of the research project that contains the data linkage component.

b) Ensure that patient identifying information obtained under paragraph (H.1) of this section is not provided to law enforcement agencies or officials.

H.3.2. *Data repositories* - For purposes of this section, a data repository is fully bound by the provisions of part 2 upon receipt of the patient identifying data and must:

a) After providing the researcher with the linked data, destroy or delete the linked data from its records, including sanitizing any associated hard copy or electronic media, to render the patient identifying information non-retrievable in a manner consistent with the policies and procedures established under §2.16 Security for records.

b) Ensure that patient identifying information obtained under paragraph (H.1) of this section is not provided to law enforcement agencies or officials.

H.4. Except as provided in paragraph (H.3) of this section, a researcher may not redisclose patient identifying information for data linkages purposes.

Reference(s):
45 CFR Part §46
45 CFR §164.508
§164.512
§164.514
42 CFR part 2 §2.52

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: De-identification of Client Information and Use of Limited Data Sets

POLICY NUMBER: 016-79-09-05

Table of Contents:

1. PURPOSE

The intent of this policy is to prescribe standards under which client information can be used and disclosed if that information can identify a person who has been removed or restricted to a limited data set. This policy describes the requirements for de-identification of client information so information cannot reasonably be used to identify the client.

2. TERMS

- ***De-Identified Information:*** client information from which YCHHS or another entity has deleted, redacted, or blocked identifiers, so that the remaining information cannot reasonably be used to identify a person (§164.514(a).

3. GENERAL PROCEDURES - *LIMITED DATA SET:* IS INFORMATION THAT EXCLUDES DIRECT IDENTIFIERS OF THE INDIVIDUAL, OR OF RELATIVES, EMPLOYERS OR HOUSEHOLD MEMBERS OF THE INDIVIDUAL (SEE SECTION (4.) BELOW FOR ADDITIONAL INFORMATION)

A. **General use of De-identified information:**

A.1. Unless otherwise restricted or prohibited by other federal or state law, YCHHS can use and share information as appropriate for the work of YCHHS, without further restriction, if YCHHS or another entity has taken steps to de-identify the information consistent with the requirements and restrictions of this policy in Section (4.)

B. **General use of Limited Data Set:**

B.1. In general YCHHS may use or disclose PHI (except for genetic test information) in a Limited Data Set for research, public health, and Health Care Operations without an individual authorization or waiver of the authorization requirement.

B.2. YCHHS may use or disclose a limited data set that meets the requirements of Section (6.) of this Policy, if YCHHS enters into a data use agreement with the limited data set recipient (or with the data source, if YCHHS will be the recipient of the limited data set) in accordance with the requirements of Section (7.) of this Policy.

4. REQUIREMENTS FOR DE-IDENTIFICATION OF CLIENT INFORMATION

A. **Determining when information is De-identified:**

A.1. YCHHS may determine that client information is sufficiently de-identified, and cannot be used to identify an individual, only if the below have occurred:

A.1.1. Removal of Identifiers: Health Information is considered de-identified if YCHHS has ensured that the following identifiers of the individual or of relatives, employers, and household members of the individual are removed and YCHHS does not have any actual knowledge that the information could be used alone or in combination with other information to identify a person (§164.514(b)(2):

a) Names;

b) All *geographic subdivisions* smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip

codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;

c) All *elements of dates* (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older;"

d) Telephone numbers;

e) Fax numbers;

f) Electronic mail addresses;

g) Social security numbers;

h) Medical record numbers;

i) Health plan beneficiary numbers;

j) Account numbers;

k) Certificate or license numbers;

l) Vehicle identifiers and serial numbers, including license plate numbers;

m) Device identifiers and serial numbers;

n) Web Universal Resource Locators (URLs);

o) Internet Protocol (IP) address numbers;

p) Biometric identifiers, including fingerprints and voiceprints;

q) Full face photographic images and any comparable images; and

r) Any other unique identifying number, characteristic, or codes, except as permitted under Section (5.), below, of this policy; **and**

A.1.2. YCHHS has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

B. **YCHHS Privacy Officer:**

B.1. The YCHHS Privacy Officer will designate the statistician or other person, with the appropriate knowledge and experience, to determine if the information referred to in (4.)(A.1.1.) above is de-identified, who may be either:

B.1.1. A YCHHS employee;

B.1.2. An employee of another governmental agency;

B.1.3. An outside contractor or consultant, subject to YCHHS contracting and personnel policy.

5. RE-IDENTIFICATION OF DE-IDENTIFIED INFORMATION

A. **Information coded for re-identification:**

A.1. YCHHS may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by YCHHS, except that:

A.1.1. The code or other means of record identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and

A.1.2. YCHHS does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification.

A.2. De-identified Health Information that has been re-identified may not be disclosed or used except as otherwise permitted under YCHHS, policy # -016-79-09-03, *Uses and Disclosures of Protected Health Information*.

6. REQUIREMENTS FOR A LIMITED DATA SET

A. **A limited data set is information that excludes the following direct identifiers of the individual, or of relatives, employers or household members of the individual: (§164.514(e)(2):**

A.1. Names;

A.2. Postal address information, other than town or city, State and zip code;

A.3. Telephone numbers;

A.4. Fax numbers;

A.5. Electronic mail addresses;

A.6. Social Security numbers;

A.7. Medical record numbers;

A.8. Health plan beneficiary numbers (such as Medicaid Prime Numbers);

A.9. Account numbers;

A.10. Certificate/license numbers;

A.11. Vehicle identifiers and serial numbers, including license plate numbers;

A.12. Web Universal Resource Locators (URLs);

A.13. Internet Protocol (IP) address numbers;

A.14. Biometric identifiers, including finger and voice prints; and

A.15. Full face photographic images and any comparable images.

7. CONTENTS OF A DATA USE AGREEMENT

A. **Disclosure of Limited Data Sets (§164.514(e):**

A.1. YCHHS may use or disclose Protected Health Information except for genetic test information in a Limited Data Set without an individual authorization or waiver of authorization, only when the following conditions are met:

A.1.1. Data Use Agreement: YCHHS has obtained a limited data set that is subject to a data use agreement, YCHHS is not restricted to using a limited data set for its own activities or operations.

A.1.2. Valid Purpose: The purpose(s) of the use or disclosure of the Limited Data Set is Research, public health or Health Care Operations; and

A.2. If YCHHS knows of a pattern or activity or practice of the limited data set recipient that constitutes a material breach or violation of a data set agreement, YCHHS will take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, YCHHS will discontinue disclosure of information to the recipient and report the problem to the United States Department of Health and Human Services (DHHS), Office of Civil Rights.

B. **Data Use Agreement (§164.514(e)(4):**

B.1. A data use agreement between YCHHS and the recipient of the limited data set must:

B.1.1. Specify the permitted uses and disclosures of such information by the limited data set recipient. YCHHS may not use the agreement to authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this Policy if done by YCHHS.

B.1.2. Specify who is permitted to use or receive the limited data set; and

B.1.3. Specify that the limited data set recipient will:

a) Not use or further disclose the information other than as specified in the data use agreement or as otherwise required by law;

b) Use appropriate safeguards to prevent use or disclosure of the information other than as specified in the data use agreement;

c) Report to YCHHS, if YCHHS is the source of the limited data set, if the recipient becomes aware of any use or disclosure of the information not specified in its data use agreement with YCHHS;

d) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

e) Not identify the information or contact the individuals whose data is being disclosed.

B.1.4. **Behavioral Health Only:** Limited data set for audit and evaluation activities. Person agrees in writing to (42 CFR Part 2, §2.53):

a) Comply with limitations on redisclosure; and

b) Destroy the entire individual's identifying information upon completion of the audit or evaluation.

C. **Exception to Accounting Requirement:** YCHHS is not required to account for its disclosure of a Limited Data Set pursuant as described in Policy #016-79-09-01, *Client Rights*. (§164.528(a)(1)(viii).

D. **Minimum Necessary Rule:** YCHHS must limit the information disclosed as described in Policy #016-79-09-06, *Minimum Necessary* information needed for the Research, public health or Health Care Operations purposes specified in the Data Use Agreement.

45 CFR 164.514 HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Minimum Necessary Information

POLICY NUMBER: 016-79-09-06

Table of Contents:

1. PURPOSE

The intention of this policy is:

- To ensure the privacy of confidential information that is used or disclosed by YCHHS employees in the course of their work; and
- To ensure that Protected Health Information (PHI) is limited to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

2. TERMS

- ***Protected Health Information (PHI):*** Is any individually identifiable health information that is:
  - Maintained electronically or on paper; or
  - Transmitted electronically, on paper, or verbally.

3. GENERAL PROCEDURES - TRANSMITTED OR MAINTAINED IN ANY OTHER FORM OR MEDIUM

A. **General Use and Disclosure (§164.502(b):**

A.1. Minimum Necessary Standard: YCHHS will use and disclose the minimum amount of information necessary to provide services and benefits to clients, and only to the extent provided by YCHHS policies and procedures. When using, disclosing, or requesting PHI, YCHHS shall make reasonable efforts to limit PHI to only the minimum necessary to accomplish the intended purpose.

A.2. The minimum necessary requirements do not apply to:

A.2.1. Client: Disclosures made to the individual about his or her own PHI;

A.2.2. Client Authorization: Uses or disclosures authorized by the individual that are within the scope of the authorization;

A.2.3. Disclosures to or requests by a health care provider for treatment:

a) **Behavioral Health Only:** This allowance under HIPAA does not apply to client substance use information protected under 42 CFR Part 2. Client authorization is required for disclosures to health care providers except in medical emergency or by court order. See policy # 016-79-09-03, *Public Health Uses and Disclosures of Protected Health Information*; Section 5. "Exceptions Allowing Limited Disclosures without Authorizations".

A.2.4. Required by Law: Uses or disclosures required by law per §164.512(a); and

A.2.5. To HHS: Disclosures to the Director, HHS HIPAA Privacy Officer, and Office for Civil Rights of the U.S. Department of Health and Human Services ("HHS"), and others for HIPAA compliance purposes per §164 subpart C.

A.2.6. Required for Compliance with HIPAA Administrative Simplification Provisions: Uses or disclosures that are required for compliance with the regulations implementing the other administrative simplification provisions of HIPAA (i.e., the transactions and code sets standard, security and electronic signature standards, etc.)

B. Entire Medical Record: As a general rule, YCHHS staff will not use, disclose or request an entire medical record of a patient unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

4. MINIMUM NECESSARY INFORMATION

A. When YCHHS policy permits use or disclosure of an individual's information to another entity, or when YCHHS requests an individual's information from another entity, YCHHS employees must make reasonable efforts to limit the amount of information to the minimum necessary needed to accomplish the intended purpose of the use, disclosure, or request.

B. Responding to Requests for Disclosures: If YCHHS policy permits making a particular disclosure to another entity, YCHHS employees may rely on a requested disclosure as being the minimum necessary for the stated purpose when: (see

below under this section more stringent requirements for client substance use information protected under 42 CFR Part 2).

B.1.1. Making disclosures to public officials that are permitted under 45 CFR 164.512, and as stated in YCHHS policy, *Uses and Disclosures of Protected Health Information*; if the public official represents the information requested is the minimum necessary for the stated purpose(s). A "public official" is any employee of a government agency who is authorized to act on behalf of that agency in performing the lawful duties and responsibilities of that agency. (See C. *Behavioral Health Only* below for compliance with 42 CFR Part 2). The information is requested by another entity that is a "covered entity" under the HIPAA Privacy rules. A "covered entity" is a health plan, a health care provider who conducts electronic transactions, or a health care clearinghouse;

B.1.2. **Behavioral Health Only:** 42 CFR Part 2 requires client authorization, except in the case of medical emergency (see YCHHS policy #016-79-09-02, *Uses and Disclosures of Protected Health Information*) or court order.

B.2. The information is requested by a professional who is a member of the workforce of a "covered entity" or is a business associate/qualified service organization of the "covered entity" for the purpose of providing professional services to the "covered entity," if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

B.3. Documentation or representations that comply with the applicable requirements of YCHHS Policy #016-79-09-04 *Uses and Disclosures for Research Purposes & Waivers* have been provided by a person requesting the information for research purposes.

C. **Behavioral Health Only**: Disclosure of client substance use information for audit and evaluation activities (42 CFR Part 2, §2.53)

C.1. Records not copied or removed*:* If patient records are not downloaded, copied, or removed from the premises, or forwarded electronically to another electronic system or device, patient identifying information may be disclosed in the course of a review of records on program premises to any person who agrees in writing to comply with the limitations on redisclosure and use in paragraph (C.6) of this section and who:

C.1.1. Performs the audit or evaluation activity on behalf of:

a) Any Federal, State, or local governmental agency which provides financial assistance to the program or is authorized by law to regulate its activities; or

b) Any individual or entity which provides financial assistance to the part 2 program or other lawful holder, which is a third-party payer covering patients in the part 2 program, or which is a quality improvement

organization performing a QIO review, or the contractors, subcontractors, or legal representatives of such individual, entity, or quality improvement organization.

c) An entity with direct administrative control over the part 2 program or lawful holder.

C.1.2. Is determined by the program director to be qualified to conduct the audit or evaluation activities.

C.2. Copying or removal of records: Records containing patient identifying information may be copied or removed from program premises by any person who:

C.2.1. Agrees in writing to:

a) Maintain and destroy the patient identifying information in a manner consistent with the policies and procedures established under §2.16;

b) Retain records in compliance with applicable federal, state, and local record retention laws; and

c) Comply with the limitations on disclosure and use in paragraph (C.6) of this section; and

C.2.2. Performs the audit or evaluation activity on behalf of:

a) Any Federal, State, or local governmental agency which provides financial assistance to the program or is authorized by law to regulate its activities; or

b) Any private person which provides financial assistance to the program, which is a third-party payer covering patients in the program, or which is a quality improvement organization performing a utilization or quality control review, or the contractors, subcontractors, or legal representatives of such individual, entity, or quality improvement organization.

c) An entity with direct administrative control over the part 2 program or lawful holder.

C.3. Activities included. Audits and evaluations under this section may include, but are not limited to:

C.3.1. Activities undertaken by a federal, state, or local governmental agency, or a third-party payer entity, in order to:

a) Identify actions the agency or third-party payer entity can make, such as changes to its policies or procedures, to improve care and outcomes for patients with SUDs who are treated by part 2 programs;

b) Ensure that resources are managed effectively to care for patients; or

c) Determine the need for adjustments to payment policies to enhance care or coverage for patients with SUD.

C.3.2. Reviews of appropriateness of medical care, medical necessity, and utilization of services.

C.4. Quality assurance entities included. Entities conducting audits or evaluations in accordance with paragraphs (C.1) and (C.2) of this section may include accreditation or similar types of organizations focused on quality assurance.

C.5. Medicare, Medicaid, or Children's Health Insurance Program (CHIP) audit or evaluation:

C.5.1. Patient identifying information, as defined in §2.11, may be disclosed under paragraph (C.5) of this section to any individual or entity for the purpose of conducting a Medicare, Medicaid, or CHIP audit or evaluation, including an audit or evaluation necessary to meet the requirements for a Centers for Medicare & Medicaid Services (CMS)-regulated accountable care organization (CMS-regulated ACO) or similar CMS-regulated organization (including a CMS-regulated Qualified Entity (QE)), if the individual or entity agrees in writing to comply with the following:

a) Maintain and destroy the patient identifying information in a manner consistent with the policies and procedures established under §2.16;

b) Retain records in compliance with applicable federal, state, and local record retention laws; and

c) Comply with the limitations on disclosure and use in paragraph (C.6) of this section.

C.5.2. A Medicare, Medicaid, or CHIP audit or evaluation under this section includes a civil or administrative investigation of a part 2 program by any federal, state, or local government agency with oversight responsibilities for Medicare, Medicaid, or CHIP and includes administrative enforcement, against the part 2 program by the government agency, of any remedy authorized by law to be imposed as a result of the findings of the investigation.

C.5.3. An audit or evaluation necessary to meet the requirements for a CMS-regulated ACO or similar CMS-regulated organization (including a CMS-regulated QE) must be conducted in accordance with the following:

a) A CMS-regulated ACO or similar CMS-regulated organization (including a CMS-regulated QE) must:

1) Have in place administrative and/or clinical systems; and

2) Have in place a leadership and management structure, including a governing body and chief executive officer with responsibility for oversight of the organization's management and for ensuring compliance with and adherence to the terms and conditions of the Participation Agreement or similar documentation with CMS; and

b) A CMS-regulated ACO or similar CMS-regulated organization (including a CMS-regulated QE) must have a signed Participation Agreement or similar documentation with CMS, which provides that the CMS-regulated ACO or similar CMS-regulated organization (including a CMS-regulated QE):

1) Is subject to periodic evaluations by CMS or its agents, or is required by CMS to evaluate participants in the CMS-regulated ACO or similar CMS-regulated organization (including a CMS-regulated QE) relative to CMS-defined or approved quality and/or cost measures;

2) Must designate an executive who has the authority to legally bind the organization to ensure compliance with 42 U.S.C. 290dd-2 and this part and the terms and conditions of the Participation Agreement in order to receive patient identifying information from CMS or its agents;

3) Agrees to comply with all applicable provisions of 42 U.S.C. 290dd-2 and this part;

4) Must ensure that any audit or evaluation involving patient identifying information occurs in a confidential and controlled setting approved by the designated executive;

5) Must ensure that any communications or reports or other documents resulting from an audit or evaluation under this section do not allow for the direct or indirect identification (e.g., through the use of codes) of a patient as having or having had a substance use disorder; and

6) Must establish policies and procedures to protect the confidentiality of the patient identifying information consistent with this part, the terms and conditions of the Participation Agreement, and the requirements set forth in paragraph (C.5.1) of this section.

C.5.4. Program, as defined in §2.11, includes an employee of, or provider of medical services under the program when the employee or provider is the subject of a civil investigation or administrative remedy, as those terms are used in paragraph (C.5.2) of this section.

C.5.5. If a disclosure to an individual or entity is authorized under this section for a Medicare, Medicaid, or CHIP audit or evaluation, including a civil investigation or administrative remedy, as those terms are used in paragraph (C.5.2) of this section, the individual or entity may further disclose the patient identifying information that is received for such purposes to its contractor(s), subcontractor(s), or legal representative(s), to carry out the audit or evaluation, and a quality improvement organization which obtains such information under paragraph (C.1) or (C.2) of this section may disclose the information to that individual or entity (or, to such individual's or entity's contractors, subcontractors, or legal representatives, but only for the purposes of this section).

C.5.6. The provisions of this paragraph do not authorize the part 2 program, the federal, state, or local government agency, or any other individual or entity to disclose or use patient identifying information obtained during the audit or evaluation for any purposes other than those necessary to complete the audit or evaluation as specified in paragraph (C.5) of this section.

C.6. Limitations on disclosure and use. Except as provided in paragraph (C.5) of this section, patient identifying information disclosed under this section may only be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by a court order entered under §2.66 of these regulations.

C.7. Audits and evaluations mandated by statute or regulation. Patient identifying information may be disclosed to federal, state, or local government agencies, and the contractors, subcontractors, and legal representatives of such agencies, in the course of conducting audits or evaluations mandated by statute or regulation, if those audits or evaluations cannot be carried out using deidentified information.

5. ACCESS & USES OF INFORMATION

A. Role Based Access: (§164.514(d)(2):

A.1. Employees of Yamhill County Health and Human Services (YCHHS) generally need access to Protected Health Information (PHI) in the performance of their positions. Each person shall only access the minimum necessary information to perform functions related to their job. YCHHS program supervisors will identify the information needed for persons, or classes of persons, in their respective workforces to carry out their duties, and will further identify any conditions appropriate to such access.

A.2. YCHHS Role-Based Access Protocol and Criteria

LEVEL 1*: None – No Access to Designated Record Set*
LEVEL 2*: May access minimum necessary PHI (not Designated Record Set) to complete assigned tasks and/or to document actions (i.e. PHI discussed)*
LEVEL 3*: Full access to the Medical Record subset of the Designated Record Set*
LEVEL 4*: Full access to the Business Office File subset of the Designated Record Set*

Position	Access Level				Explanation/Duties Performed Requiring Access
	1	**2**	**3**	**4**	
Billing/Insurance Staff		x		x	Operations/Payment
Business Associates		x			Per BA Agreement
Business Services/Contract Management Staff		x		x	Operations/Payment
Contractors		x			Per Contract
Core Staff		x	x		Treatment
Clinical (including: CADC, Techs, Peer Specialist, QMHA, QMHP, RN, LMP)		x	x	x	Treatment
Clinical Student		x	x	x	Treatment
Director		x	x	x	
Electronic Health Record Staff		x	x	x	Operations/Payment
Emergency Preparedness & Health Promotion Staff	x				
Environmental Health Staff	x				
Finance/Analytics Staff		x		x	Operations/Payment
Managers/Supervisors		x	x	x	Treatment/Operations/Payment
Privacy Official		x	x	x	Treatment/Payment/Operations
Veterans Staff	x				
Volunteers	x				

B. **Routine and Recurring Disclosure of an Individual's Information:(§164.514(d)(3)(i) and Oregon DHS policy DHS-100-004, July 2009):**

B.1. For the purposes of this policy, a "routine and recurring" means the disclosure of records outside YCHHS, without the authorization of the individual, for a purpose that is compatible with the purpose for which the information was collected. The following identifies several examples of uses and disclosures that YCHHS has determined to be compatible with the purposes for which information is collected (45 CFR §5b.1(j).

B.1.1. YCHHS will not disclose an individual's entire medical record unless the request specifically justifies why the entire medical record is needed.

B.1.2. Routine and recurring uses include disclosures required by law. For example, a mandatory child abuse report by a YCHHS employee would be a routine use.

B.1.3. If YCHHS deems it desirable or necessary, YCHHS may disclose information as a routine and recurring use to the Oregon Department of Justice for the purpose of obtaining its advice and legal services.

B.1.4. When federal or state agencies – such as the DHHS Office of Civil Rights, the DHHS Office of Inspector General, the State of Oregon Medicaid Fraud Unit, or the Oregon Secretary of State – have the legal authority to require YCHHS to produce records necessary to carry out audit or oversight of YCHHS programs or activities, YCHHS will make such records available as a routine and recurring use.

B.1.5. When the appropriate YCHHS official determines that records are subject to disclosure under the Oregon Public Records Law, YCHHS may qualify the disclosure as a routine and recurring use.

B.2. YCHHS Established Routine or Recurring Disclosures for HIPPA (alcohol and drug records, under 42 CFR Part 2) requires client authorization, except in the case of medical emergency, see YCHHS Policy #016-79-09-02, *Uses and Disclosures of Protected Health Information*, or court order.

Requester	Purpose	Disclosures
Disability Determination	Evaluate individual's medical condition in support of disability benefits	Specific information requested
Department of Community Justice	Coordination of Services	All Behavioral Health and Medical Records as requested
DHS Child Welfare	Coordination of Services Mandatory abuse reporting	All Behavioral Health and Medical Records as requested
Emergency Contact	Emergency Needs	Emergency medical information
Healthcare oversight agency	Investigate a complaint	Protected health information related to complaint
Insurance Company	Substantiate care provided for payment To bill for services rendered under Medical insurance coverage and obtain any authorization necessary	Specific information requested in claims attachment request
Juvenile Department	Coordination of Services To verify compliance or non-compliance	Diagnostic Impression and Diagnosis Prognosis and Treatment Recommendations

Law enforcement	To locate a fugitive, missing person, material witness or suspect of a crime	Per response to criteria and review committee decisions *may include:* • Name and address • Date and place of birth • Social security # • ABO blood type • Type of injury • Date and time of treatment • Date and time of death • Description of physical characteristics **DO NOT DISCLOSE ANY DNA analysis, dental records or typing, sample of analysis of body fluids**
Life Insurance	Evaluate individual's medical condition for issuance of a life insurance policy	Discharge summaries for specified period of time
Medical provider/PCP/Clinic	Coordination of Services	All Behavioral Health and Medical Records as requested
Oregon Department of Justice	Obtaining its advice and legal services	
Parents (DD)	To determine eligibility for county DD services	Any information related to eligibility and services
Pharmacy	Obtain demographic and insurance information for billing	Face sheet with patient demographics, diagnoses and insurance information
Potential Employers	Coordination of Services	Abacus Program Description
School District	Coordination of Services	Academic Testing
Transportation	Transportation Coordination	Appointment dates, time and status
Vocational Rehabilitation	Coordination of Services	Abacus Program Description
Willamette Education Service District	Coordination of Services	All medical records as requested
WIC	Coordination of Services	All medical records as requested
Social Services Agencies working with a shared client	Coordination of Services	All medical records as requested
Yamhill Community Care Organization	Coordination of Services	All medical records as requested
Yamhill County Probation	Coordination of Services To verify compliance or non-compliance	All medical records as requested

6. NON-ROUTINE DISCLOSURE OF AN INDIVIDUAL'S INFORMATION

A. For the purpose of this policy, "non-routine disclosure" means the disclosure of records outside YCHHS that are subject to the minimum necessary requirement and have not been approved as routine and recurring per YCHHS HIPAA Manual Subject: Minimum Necessary 5(B) (§164.514(d)(3)(ii).

B. Requests for non-routine disclosures must be reviewed on an individual basis.

C. For Non-Routine Disclosures, YCHHS program areas will:

C.1. Limit the PHI disclosed to the amount reasonably necessary to accomplish the purpose of the disclosure or request;

C.2. Not use or disclose an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request (§164.514(d)(5).

C.3. The YCHHS HIPAA Privacy Officer or designee will review requests for non-routine disclosures on an individual basis based on the following criteria:

C.3.1. The identity and authority of the requester;

C.3.2. The purpose of the request or disclosure;

C.3.3. The nature and extent of information requested;

C.3.4. To determine if authorization can reasonably be obtained from the individual or personal representative;

C.3.5. The extent to which requested Protected Health Information can be extracted from the rest of the medical record without undue burden and without viewing unnecessary parts of the record;

C.3.6. Where the Protected Health Information will be viewed or used;

C.3.7. The availability of physical, technical and other security measures at the place of viewing or use;

C.3.8. To determine if the purpose could be achieved by providing de-identified information (see YCHHS policy #016-79-09-05, *De-identification of Client Information and Use of Limited Data Sets);*

C.3.9. The trustworthiness of the person who will access or use the Protected Health Information.

7. YCHHS' REQUEST FOR AN INDIVIDUAL'S INFORMATION FROM ANOTHER ENTITY

A. When requesting information about an individual from another entity, YCHHS employees must limit requests to those that are reasonably necessary to accomplish the purpose for which the request is made.

A.1. YCHHS will not request an individual's entire medical record unless YCHHS can specifically justify why the entire medical record is needed. (§164.514(d)(5).

8. GUIDANCE FOR PROCEDURE DEVELOPMENT

The following guidelines should be used in developing procedures to implement this policy:

A. **Disclosures of an Individual's Information on a routine or recurring basis.** For Routine and Recurring Disclosures, YCHHS program areas will:

A.1. Determine who is requesting the information and the purpose for the request;

A.1.1. If the request is **not** compatible with the purpose for which it was collected, refer to and apply the "non-routine use" procedures in the following section.

A.2. Confirm that the applicable YCHHS policies and program rules permit the requested use (disclosure is consistent with the program purposes), and that the nature or type of the use recurs (occurs on a periodic basis) within the program or activity;

A.3. Identify the kind and amount of information that is necessary to respond to the request; and

A.4. If the disclosure is one that must be included in the YCHHS accounting of disclosures, include required documentation in the accounting log. For further information on what disclosures need to be accounted for, see YCHHS policy #016-79-09-01, *Client Rights* or the YCHHS Form #1021, *Accounting of Disclosures Log*.

B. **Disclosures of an Individual's Information on a non-routine basis:** For non-routine disclosures, YCHHS divisions and program areas will:

B.1. Determine who is requesting the information and the purpose for the request;

B.1.1. If the request **is** compatible with the purpose for which it was collected, apply the "routine and recurring use" procedures in the previous section.

B.2. Determine which information of the individual is within the scope of the request, and what YCHHS policies and program rules apply to the requested use;

B.3. If the information requested can be disclosed under the applicable program and HIPAA policies, limit the amount of information to the minimum amount necessary to respond to the request; and

B.4. Document the disclosure in the accounting log.

Reference(s): 45 CFR Parts 160 and 164

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Business Associate Relations & Qualified Service Organizations

POLICY NUMBER: 016-79-09-07

Table of Contents:

1. PURPOSE

The purpose of this policy is to ensure that Yamhill County Health and Human Services (YCHHS) Business Associates/Qualified Service Organization (as defined below) protect patients' right to privacy. This policy specifies when YCHHS may disclose an individual's protected health information (PHI) to a business associate of YCHHS, and to specify provisions that must be included in YCHHS contracts with business associates.

2. TERMS

- ***Business Associate (HIPAA)/Qualified Service Organization (42 CFR part 2):*** An individual or corporate "person" who: On behalf of Yamhill County performs any function or activity involving the use or disclosure of protected health information (PHI); and is *not* a member of Yamhill County's workforce.
  - The definition of "function or activity" includes: claims processing or administration, data analysis, utilization review, quality assurance, billing, legal, actuarial, accounting,

consulting, data processing, management, administrative, accreditation, financial services and similar services for which the Department might contract, if access to PHI is involved.

- Business associates/qualified service organizations do not include Licensees or Providers unless the Licensee or Provider also performs some "function or activity" on behalf of YCHHS.

❖ ***Designated Record Set:*** (1) individuals' medical records, (2) any YCHHS billing records concerning individuals, and (3) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan.

1. For purposes of this definition, *"record"* means any item, collection or grouping of information that includes individually identifiable health information and is maintained, collected, used, or disseminated by or for YCHHS and is used, in whole or in part, by or for the YCHHS to make decisions about individuals.

❖ ***Individually Identifying Information:*** Any single item or compilation of information or data that indicates or reveals the identity of an individual, either specifically (such as the individual's name or social security number), or that does not specifically identify the individual but from which the individual's identity can reasonably be ascertained.

❖ ***Protected Health Information (PHI):*** Any individually identifiable health information, whether oral or recorded in any form or medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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. Any data transmitted or maintained in any other form or medium by covered entities, including paper records, fax documents and all oral communications, or any other form, i.e. screen prints of eligibility information, printed e-mails that have identified individual's health information, claim or billing information, hard copy birth or death certificate.

2. ***Protected health information excludes***: school records that are subject to the Family Educational Rights and Privacy Act; and employment records.

❖ ***Workforce:*** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for YCHHS is under the direct control of YCHHS, whether or not they are paid by YCHHS.

3. GENERAL PROCEDURES

A. **Applicability of a Business Associate Relationship:**

A.1. Not all contractors or business partners are "business associates" of YCHHS. This policy only applies to contractors or business partners that come within the definition of a "business associate."

A.2. If a contractor or business partner is a "business associate," they will be subject to all federal and state laws and policies governing the contractual relationship. A "business associate" relationship also requires additional contract provisions. The additional contract requirements are described in Section 4 below.

B. **Definition of Business Associate:** "Business Associate" means (§160.103)

B.1. With respect to YCHHS, a person who:

B.1.1. On behalf of YCHHS, (not including the workforce of YCHHS), performs or assists in the performance of:

a) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

b) Any other function or activity regulated by federal regulations at 45 CFR Subtitle A, Subchapter C; or

B.1.2. Provides, (other than in the capacity of the YCHHS workforce), legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for YCHHS, or for an organized health care arrangement in which YCHHS participates, where the provision of the service involves the disclosure of individually identifiable health information from YCHHS, or from another business associate of YCHHS, to the person.

B.2. A business associate relationship is formed only if protected health information is to be used, created, or disclosed in the relationship.

B.3. A covered entity may be a business associate of another covered entity.

C. **The Following are not Business Associates:**

C.1. The workforce of YCHHS;

C.2. Health care providers providing treatment to individuals which, YCHHS discloses Protected Health Information in connection with the treatment of a client; or

C.3. A vendor that places its employees on YCHHS's premises to the extent that the employees perform a substantial proportion of their activities at such location and YCHHS treats such employees as members of its Workforce for the purpose of complying with the Privacy Rule;

C.4. Enrollment or eligibility determinations, involving YCHHS clients, between government agencies;

C.5. Payment relationships, such as when YCHHS is paying medical providers, childcare providers, OHP managed care organizations, or other entities for services to YCHHS clients or participants, when the entity is providing its own normal services that are not on behalf of YCHHS;

C.6. When an individual's protected health information is disclosed based solely on an individual's authorization;

C.7. When an individual's protected health information is not being disclosed by YCHHS or created for YCHHS; and

C.8. When the only information being disclosed is information that is de-identified in accordance with YCHHS policy # 016-79-09-05, *De-identification of Client Information and Use of Limited Data Sets*.

D. YCHHS may disclose an individual's protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit an individual's protected health information on behalf of YCHHS, if the contract includes the language outlined below under *(4.) Contract Requirements Applicable to Business Associates* (§164.308(b); and 164.314(a).

E. **Definition of Qualified Service Organization in relation to alcohol and drug treatment records: "**Qualified Service Organization" means (per 42 CFR part 2 §2.11) a person which:

E.1. Provides services to a program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and childcare and individual and group therapy; and

E.2. Has entered into a written agreement with a program under which that person:

E.2.1 Acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the programs, it is fully bound by these regulations; and

E.2.2 If necessary, will resist in judicial proceedings any efforts to obtain access to patient records except as permitted by these regulations.

4. CONTRACT REQUIREMENTS APPLICABLE TO BUSINESS ASSOCIATES

A. **Permitted and Required Uses and Disclosures (§164.504(e)(2):** The Business Associate Contract must specify and describe the permitted and required uses and disclosures of Protected Health Information by the Business Associate or Qualified Service Organization. The written contract or agreement between YCHHS and the Business Associate or Qualified Service Organization may permit the Business Associate or Qualified Service Organization to (164.504(e):

A.1. **Use information** it receives in its capacity as a business associate or qualified service organization to YCHHS, if necessary:

A.1.1. For proper management and administration of the business associate or qualified service organization; or

A.1.2. To carry out the legal responsibilities of the business associate or qualified service organization; or

A.1.3. To collect data relating to YCHHS operations.

A.2. **Disclose information** it receives in its capacity as a business associate if:

A.2.1. The disclosure is required by law; or

A.2.2. The business associate receives assurances from the person to whom the information is disclosed that:

a) It will be held or disclosed further only as required by law or for the purposes to which it was disclosed to such person; and

A.3. The person notifies the business associate or qualified service organization of any instances or any known instances in which the confidentiality of the information has been breached.

A.4. The contract may not authorize the business associate or qualified service organization to further use or disclose health information obtained from YCHHS.

B. **The Agreement must also provide that the business associate or qualified service organization will:**

B.1. ***Not use or further disclose*** protected health information other than as permitted or required by the contract or as required by law;

B.2. ***Safeguards by Business Associate:*** Use appropriate safeguards to prevent, use, or disclosure of the information other than as provided for by the contract;

B.3. ***Reporting by Business Associate:*** Report to YCHHS any use or disclosure not allowed by the contract of which the business associate becomes aware, including breaches of unsecured protected health information as required by 164.410;

B.4. ***Subcontractors:*** Ensure that any agents or subcontractors to whom it provides protected health information agrees to the same restrictions and conditions that apply to the business associate under the contract;

B.5. ***Inspection and Copying:*** Make protected health information available to the individual in accordance with YCHHS policy # 016-79-09-01 *Client Rights*;

B.6. ***Amendments:*** Make protected health information available for amendment and incorporate any amendments in accordance with YCHHS, YCHHS policy # 016-79-09-01 *Client Rights*;

B.7. ***Accounting of Disclosures:*** Make available the information required to provide an accounting of disclosures in accordance with YCHHS policy # 016-79-09-01 , *Client Rights*;

B.8. ***Inspection:*** Makes its internal practices, books, and records relating to the use and disclosure of protected health information available to YCHHS and to the United States DHHS for the purpose of determining YCHHS compliance with federal requirements; and

B.9. ***Termination and Return of PHI:*** At termination of the contract, if reasonably feasible, return or destroy all protected health information that the business associate still maintains in any form, and keep no copies thereof. If not feasible, the business associate will continue to protect the information.

B.10. ***Termination for Material Breach:*** Authorize termination of the contract if YCHHS determines that the business associate has violated a material term of the contract.

5. BUSINESS ASSOCIATE OR QUALIFIED SERVICE AGREEMENT WITH ANOTHER GOVERNMENT ENTITY

A. **If the Business Associate or Qualified Service Organization of YCHHS is Another Governmental Entity (164.504(e)(3):**

A.1. YCHHS may enter into a memorandum of understanding, rather than a contract, with the business associate if the memorandum of understanding contains terms covering all objectives of (4.) *Contract Requirements Applicable to Business Associates*, above, of this policy;

A.2. The written contract, agreement, or memorandum does not need to contain specific provisions required under (4.) *Contract Requirements Applicable to Business Associates*, above, if other law or regulations contain requirements applicable to the business associate that accomplish the same objective;

B. If a Business Associate or Qualified service organization is required by law to perform a function or activity on behalf of YCHHS, or to provide a service to YCHHS, YCHHS may disclose protected health information to the business associate or qualified service organization to the extent necessary to enable compliance with the legal requirement, without a written contract or agreement, if:

B.1. YCHHS attempts in good faith to obtain satisfactory assurances from the business associate that the business associate or qualified service organization will protect health information to the extent specified in (4.) *Contract Requirements Applicable to Business Associates*, above; and

B.2. If such attempt fails, YCHHS documents the attempt and the reasons that such assurances cannot be obtained;

6. RESPONSIBILITIES OF YCHHS IN BUSINESS ASSOCIATE AND QUALIFIED SERVICE ORGANIZATION RELATIONSHIPS

A. **YCHHS Responsibilities in business associate or qualified service organization relationships include, but are not limited to, the following:**

A.1. Receiving and logging an individual's complaints regarding the uses and disclosures of protected health information by the business associate/qualified service organization or the business associate/qualified service organization relationship (§164.308(a)(6)(i); §164.408(c);

A.2. Receiving and logging reports from the business associate/qualified service organization of possible violations of the business associate contracts;

A.3. Implementation of corrective action plans, as needed; and

A.4. Mitigation, if necessary, of known violations up to and including contract termination.

B. **Consultation:** YCHHS will provide business associates/qualified service organizations with applicable contract requirements and may provide consultation to business associates as needed on how to comply with contract requirements regarding protected health information.

7. BUSINESS ASSOCIATE NON-COMPLIANCE

A. **Material Breach (164.504(e)(1)(ii)(iii):**

A.1. If YCHHS knows of a pattern of activity or practice of a business associate/qualified service organization that constitutes a material breach or violation of the business associate's obligation under the contract or other

arrangement, YCHHS must take reasonable steps to cure the breach or end the violation, as applicable, including working with and providing consultation to the business associate/qualified service organization.

B. **If such steps are unsuccessful, YCHHS must:**

B.1. Terminate the contract or arrangement, if feasible; or

B.2. If termination is not feasible, report the problem to the United States DHHS.

8. GUIDANCE FOR PROCEDURE DEVELOPMENT

A. **Tracking and identifying YCHHS' Business Associates /Qualified Service Organizations:**

A.1. YCHHS will identify those business relationships that are also Business Associates or Qualified Service Organizations. Contract database maintained by YCHHS Administrative Services.

A.2. YCHHS will include legally appropriate "business associate/qualified service organization" contract terms and conditions in such contracts, which may include incorporation by reference to administrative rule.

B. **YCHHS' response to complaints about Business Associates or Qualified Service Organizations inappropriate uses or disclosures:**

B.1. YCHHS staff who receive a client complaint, or a report or complaint from any source, about inappropriate uses or disclosures of information by business associates/qualified service organizations, will:

B.1.1. Provide information regarding that report or complaint to the YCHHS Privacy Officer, who will document such information in the business associate's /qualified service organizations contract record maintained by YCHHS Administrative Services;

B.2. The YCHHS Privacy Officer will send a letter or email to the business associate/qualified service organization, requesting that the business associate/qualified service organization review the circumstances related to the alleged pattern or practice. YCHHS will require that the business associate respond, in writing, within 10 business days to the complaint.

B.3. The YCHHS Privacy Officer will coordinate with the business associate's/qualified service organization's YCHHS contract administrator to document the alleged violation.

B.3.1. If determined necessary and appropriate, YCHHS Administrative Services will generate a "cure letter" outlining required remediation in order for the business associate/qualified service organization to attain contract compliance.

B.4. In cases where contract compliance cannot be attained, YCHHS must terminate the contract, if feasible. If termination is not feasible, the YCHHS Privacy Officer will report the problem to the United States DHHS, Office of Civil Rights.

Reference(s): 45 CFR 160 & 164; 45 CFR §164.502(e); 42 CFR Part 2 § 2.11

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Administrative Safeguards 45 CFR §164.308

1.1. POLICY NUMBER: 016-79-09-08

Table of Contents

1. PURPOSE

It is the policy of YCHHS that all personnel preserve the integrity and confidentiality of health and other sensitive information pertaining to Yamhill County clients. The purpose of this policy is to ensure that YCHHS has the systems, policies and procedures to prevent, detect, contain and correct security violations.

2. TERMS

- **Physical Safeguards** are administrative actions, and policies and procedures, to manage the

selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information (§164.304).

- **SFTP** means Secure File Transfer Protocol (also known as SSH File Transfer Protocol). It is a network protocol that provides file access, file transfer, and file management over any reliable data stream.

3. SECURITY MANAGEMENT PROCESS

A. **Risk Analysis:**

A.1. The YCHHS HIPAA Privacy Officer or designee will perform an annual risk assessment, or whenever there are significant changes to the information system or environment of operation that may impact the security of the YCHHS system, to assess threats, vulnerabilities, likelihood, and impact on the organization.

A.1.1. The annual risk assessment will be performed using the Office of National Coordinator for Health Information Technology (ONC) Security Risk Assessment or comparable tool.

A.2. The YCHHS HIPAA Privacy Officer will review results of the risk assessment and as deemed necessary, develop an action plan to address and eliminate as reasonably possible the threats and vulnerabilities identified.

A.3. The YCHHS HIPAA Privacy Officer will distribute results of the risk assessment and action plan to YCHHS leadership as applicable.

A.4. Risk assessment and action plan will be maintained per record retention requirements.

B. **Risk Management:**

B.1. Security Plan:

B.1.1. Operational environment for the information system and relationships with, or connections to, other information systems:

Microsoft Active Directory manages the Yamhill County file system and all of the user accounts for network logons, network groups, and associated network access rights components. Everything else is a layer on top of that. The layer below that is the configuration for all the switches and routers in addition to the basic operating system functions of the servers.

B.1.2. Overview of the security requirements for the system. The security requirements are both outward and inward; with different focus.

a) The outward facing is to block rogue software or unauthorized users to gain access through the Yamhill Count IT outer defenses.

b) The internal is for configuring user rights so that the legitimate user community has access and capabilities that exactly match their job function and no more. That also includes internal functions such as allowing an

internet uplink inside the Yamhill County wireless network for non-county computers but directing them to the internet gateway only.

B.1.3. Security controls in place or planned for meeting those requirements, including a rationale for the tailoring decisions:

Documenting most of this is in the planning stages – there are many security controls in place, however, there is not a manual or policy yet that specifies the framework of those controls.

B.1.4. Security-related activities:
Yamhill County IT periodically hires contractors to hack the Yamhill County network and do a security assessment using sophisticated tools, which expose weaknesses in the Active Directory implementation or in outwardly facing security components. This provides Yamhill County a third-party security assessment document used by Yamhill County IT to address gaps in the security system and mitigate future risk.

C. **Sanction Policy**: See HIPAA Manual policy #016-79-09-11, *Enforcement, Sanctions, and Penalties for Violations of Individual Privacy*

D. **Information System Activity Review:**

D.1. Electronic Health Record (i.e., Juniper) and Yamhill County Information Technology (IT) audit capabilities:

D.1.1. Yamhill County IT: The focus is on prevention of unauthorized access, including:

a) Locking an account after three unsuccessful logon attempts prevents repeatedly guessing a password if a user account is known.

b) Logon screens do not display the previously used logon name, so an intruder would need both a user account and password to gain unauthorized access.

c) Firewall logs identify all unsuccessful logons, what was attempted, and what address the logon attempts originated from.

d) Use of two-factor authentication (DUO) for all hardware and additionally for Windows licenses.

D.1.2. Electronic Health Record:

a) Three repeated incorrect logon attempts will lock an account. Audit capabilities on the database are limited to events that range from attempting to gain access to the system through all aspects of system usage, including which particular records or clients were accessed.

b) Limit functions assigned to a particular logon. Groups that bundle database access rights are assigned to individual user accounts. Most user accounts have a clinical or a program support focus. The groups are constructed to minimize the capabilities of a user while supporting all necessary functions. The threat posed by giving excessive database rights to the user community creates vulnerability due to malicious or accidental behavior. The more

limited the user rights, the less downside risk from mistakes or purposeful damage.

c) Access Controls:

When a user has gained access to the system the primary mechanism for preventing unauthorized access is to set up a client for "access control". That administrative feature either blocks access to open a client record or requires the user to provide a specific reason for accessing the account. Those "break the glass" events can be audited (See 5. Workforce Security, A.5.below).

D.2. Audit and Monitoring Capabilities:

D.2.1. Monitoring account usage:

a) Specific requests to the EHR team are required at the present time and would need to include specific issues and time frames for the EHR team to create a report.

b) In real time, EHR staff can review all currently active users and determine what screen they are on, what client they are viewing, and how much system resource they are using. That is generally used for support purposes only but on occasion a session may need to be terminated for using excessive system resources.

c) In the forensic context, logs of system activity can reconstruct after the fact all aspects of system usage such as client records viewed and what time is associated with any of those events.

D.2.2. Remote access: Granted through supervisor approval and setup by Yamhill County IT. The Yamhill County IT Division manages all aspects of controlling access and auditing usage of the remote desktop server, which uses two-factor authentication. Remote access for e-mail is accomplished using Outlook Web Access client, which is a secure website requiring full logon credentials.

D.2.3. Wireless connectivity: Connections to the network with a county-owned computer, whether wireless or not, require full authentication. That includes confirmation that the device already belongs to the network domain. If a device connects that is not joined to the network domain, only Internet access is allowed.

D.2.4. Mobile Device Configuration: Laptops, tablets, and smart phones can all connect to county resources. The security configuration and limitations are primarily based on the user account requesting access from a mobile device, and are managed by Yamhill County IT.

D.2.5. Configuration Settings: Yamhill County IT is responsible for security configurations and monitoring of behavior of connected devices. There are several levels of control, including the firewall, anti-malware software, anti-virus software, and Untangle security software. When county computers connect to the domain, web site domain restrictions are downloaded to the local device. That means if someone disconnects from the county network and finds a local

hotspot at a public place, the same internet restrictions are in place as when connected to the network.

D.2.6. System component inventory: Yamhill County IT is responsible to configure, maintain and assure the reliability of all levels of system architecture. That includes both hardware and software inventory management, in addition to maintaining proper licensing and maintenance fees associated with components.

D.2.7. Physical Access (See policy #016-79-09-09, *Physical Safeguards*):

a) Yamhill County IT is responsible for maintaining access permissions based on scanning of an employee badge to gain entry to buildings and facilities managed by the county. Whether an employee needs to be allowed into only one building between 8am and 5pm or around the clock access to any building, an employee badge is configured to achieve the necessary level of access.

b) Other physical access issues involve physical keys that are checked out to employees as needed, usually for office doors.

c) Areas where workforce members work with medical records are restricted based on gaining entry to an "employees only" area through a card-key access door where the public is not allowed unless escorted by a county employee.

D.2.8. Temperature and humidity are of concern only in the server room that Yamhill County IT manages where air conditioning is essential and a temperature of around 70 degrees is maintained at all times.

D.2.9. Equipment Delivery and Removal:

a) Yamhill County IT manages the installation, maintenance, and eventual removal of electronic devices, including desktop computers, laptops, computer notebooks and tablets, scanners and printers. If a device with internal storage is taken out of service or re-deployed, the process includes a US Department of Defense (DoD) level multi-faceted wiping of disk resident files with repeated over-writes based on clearing and sanitizing standard DoD 5220.22-M. This assures that the original contents of the computer have been rendered unrecoverable.

b) YCHHS is responsible for managing the deployment and removal of copy machines, fax machines and smart phones (See policy #016-79-09-09, *Physical Safeguards*).

D.3. The YCHHS HIPAA Privacy Officer and/or designated YCHHS Administrative Services staff will, request, review and analyze the information system audit records and develop an action plan to address and eliminate as reasonably possible the threats and vulnerabilities identified.

D.4. The YCHHS HIPAA Privacy Officer and/or designated YCHHS Administrative Services staff will distribute results of the information systems audit and action plan to YCHHS leadership as applicable.

D.5. Audit results and action plan will be maintained per record retention requirements.

4. ASSIGNED SECURITY RESPONSIBILITY

A. The YCHHS Director will designate the YCHHS HIPAA Privacy Officer responsible for YCHHS protected health information security. The HIPAA Privacy Officer will collaborate closely with:

A.1. The YCHHS Administrative Services Director responsible for oversight, management, and security of the YCHHS electronic health record and YCHHS data base; and

A.2. The Yamhill County Information Technology Division manager

5. WORKFORCE SECURITY

A. Authorization and/or Supervision:

A.1. The YCHHS Administrative Services Director (i.e., Accounts Manager) or designee is responsible for:

A.1.1. Information System Accounts Management (Information system account types include, Ahlers Clinical Visit Record; ALERT Immunization Information System (ALERT IIS); Clinical Integration Manager (CIM); Electronic Health Record; E-Prescribing Software; Express Payment & Reporting System (eXPRS); Medicaid Management Information System (MMIS); One Health Port; and SFTP Network drives/folders).

A.1.2. Conditions for group and role membership per EHR capability, SFTP sites, etc.:

a) System access is authorized and enabled on a case-by-case basis. User rights profiles are assigned by group membership designed to minimize access to the lowest level that enables all necessary functionality. EHR system user accounts are disabled immediately if someone leaves the organization, but are left as a disabled account instead of removing in order to assure that system activity history that contains a particular user account properly links to the associated account.

b) For systems outside EHR, administration responsibilities belong to either Yamhill County IT or an outside entity such as the State of Oregon, Yamhill Community Care (YCC), Performance Health Technology (PHTech), or any number of partners for which a contract or memorandum of understanding (MOU) exists.

1) For example, SFTP access is enabled for PHTech to send eligibility file updates. YCHHS uses the PHTech site for eligibility files only.

A.1.3. Create, enable, modify, disable, and remove information system:

a) For the EHR system, user accounts are created based on submission of a formal employee request form. Once management has approved the authorization, a user account is created as needed to support the approved job function. Most requests to modify existing accounts are handled by the

EHR support team and typically involve changing business needs or workforce members focus requiring an edit to the level of system access authorized. An exception to that may be the accounting staff opening up a provider to a new cost center based on billing-related rationale. EHR system user accounts are disabled immediately if someone leaves the organization, but are left as a disabled account rather than being removed for audit purposes.

b) For information system accounts outside the EHR, administrative responsibility belongs to either the Yamhill County IT Division or an outside agency such as the State of Oregon or other outside system administrator.

A.1.4. Monitor the use of information system accounts:

a) For the EHR system, monitoring means:

1) Formal monitoring of system activity that includes:

i. Security events - tracks logins, user account modifications;

ii. Patient record access - tracks all edits and views of patient related data; and

iii. Table operations - import and export of data, backup and restore operations.

2) Use of an EHR system logon conveys acceptance of responsibility for HIPAA compliance and adherence to data security guidelines while logged in to the EHR. It may be possible, for example, to view a restricted client record. The logged-in user would be required to provide a reason why viewing the restricted record is necessary. The system will allow access, but the reason the user provides is tracked and becomes part of the audit trail.

3) Informal monitoring via day-to-day operational review is primarily around assuring that the system is running properly. That includes the ability to monitor all current logons connected to the EHR system in real time.

A.1.5. Authorized access to the information system based on:

a) A valid access authorization requires an industry standard user account and password pairing. Strong passwords are required in order to change a password that complies with the minimum requirements outlined in the document titled, Creating a *STRONG PASSWORD*, located on the HHS intranet.

b) Intended system usage pertains to the "profile" established for a user account, with valid access authorization approved by management as a prerequisite.

c) Other attributes as required by YCHHS:

1) Special case circumstances exist for third party agencies that may use the EHR system for billing purposes and clinical documentation to assure continuity of client care.

i. For example, case management responsibilities may be shared between organizations such as Provoking Hope and YCHHS.

2) Authorization is provided by management on a case-by-case basis. MOUs exist between the two parties, and EHR accounts are then set up for remote access from the third party agency.

A.1.6. Review accounts for compliance with account management requirements:
User account setup based on documentation submitted by a supervisor creates a user profile and enables a new user to access the production system after training. Supervisors occasionally revise what the requirements are for a particular staff member and submit those requests on a change form. When an employee leaves the organization, another form is submitted indicating that the staff member has terminated employment. At that point, the login account is immediately disabled. User accounts are not deleted since only the user account ID is included in the various audit logs.

A.1.7. Process for reissuing shared/group account credentials (if deployed) when individual is removed from the group:
Shared or "group" account credentials are a security vulnerability and are avoided. It is essential to have each account linked to a particular individual who is responsible for all activity using that account. Staff members are not allowed to share their logons or to log in as someone else. Groups are used to assign collective rights to an individual, not to enable a group of people to log in under the same user account.

A.2. YCHHS supervisors or designees will:

A.2.1. Complete the YCHHS Employee Set-up or Change Form and submit as instructed to request access to accounts required for the individual to perform needed operations on YCHHS information systems.

A.2.2. Notify account managers:

a) When accounts are no longer required;

b) When users are terminated or transferred;

c) When individual information system usage or need-to-know changes.

A.3. YCHHS supervisors or designee will complete the YCHHS Employee Set-up or Change Form and submit as instructed for all new workforce members requesting access permission to accounts required for the individual to perform needed operations on YCHHS information systems.

A.4. YCHHS grants all workforce members access to the YCHHS electronic health record and train on the minimum necessary standard.

A.5. The YCHHS electronic health record allows for some limited access controls at the individual client level per provider or individual client request. The Raintree Access Control List (ACL) feature is set up to provide two tiers of patient-level information restrictions for special handling.

A.5.1. Break the Glass: When activated for a client it requires the user to provide a

specific reason for accessing a client account based on whatever criterion are deemed appropriate by administrative management. Those events are part of the audit log and the explanation contained in a confidential log maintained by administration.

a) Even workforce members with the EACCESS=E security right defined must still provide a specific reason for accessing client data where the client has been flagged for ACL, which generally means one time a day a reason for access is required and any subsequent access to the same client on the same day is allowed without a reason.

A.5.2. Limited to ACL only: If this setting is made on the client record then ONLY the workforce members specifically granted access are allowed to view the client record. That would usually mean a case manager and other treatment team members would be the only workforce member set up to view the client record.

A.5.3. There is a special case feature that allows administration to restrict access to a client record by a Juniper user account, even if no access control is defined in the patient demographic record. A particular user in Juniper can be blocked from accessing a client record by explicitly restricting access for that user, e.g., a relative of a client receiving services who works for the organization.

A.6. The YCHHS electronic health record allows for limited access controls based on group or category of users, for example, business associates or contract workforce members.

A.7. See policy #016-79-09-09, *Physical Safeguards*, for access controls related to client hard copy records and digital media.

A.8. Access agreement for non-workforce members as documented in:

A.8.1. Business Associate Agreements

A.8.2. Contractor agreements

B. **Termination Procedures for Separating Workforce Member**:

B.1. Per the Yamhill County Courthouse Keys policy, Yamhill County employee separation procedures, and the YCHHS Separating Employee Instructions/Form, Yamhill County will:

B.1.1. Disable information system access;

B.1.2. Revoke any authenticators/credentials for the separating workforce member;

B.1.3. Retrieve all security-related organizational information system-related property;

B.1.4. Retain access to organizational information and information systems formerly controlled by the terminated individual;

B.1.5. Notify responsible person(s) per policy and or separating employee instructions; and

B.1.6. Conducts exit interviews that will ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security

topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment.

a) See YCHHS Exit Interview Questions document.

C. Transfer and Reassignment Procedures:

C.1. YCHHS supervisors or designees will complete the YCHHS Employee Set-up or Change Form and submit as instructed noting any changes required to access permissions in response to transfer or reassignment of duties.

C.2. YCHHS Supervisor and/or designee will review the workforce member's ongoing operational need for current access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization. This will include review of:

C.2.1. Keys;

C.2.2. Electronic key card access permissions;

C.2.3. Access to accounts, including those listed above under "A" above.

6. INFORMATION ACCESS MANAGEMENT

A. Access Authorization:

A.1. See #5 above.

A.2. Separation of Duties:

A.2.1. Information system access authorization is a shared responsibility between Yamhill County Information Technology Division and YCHHS Administrative Services.

A.2.2. Electronic Health Record access authorization is a shared responsibility within the Electronic Health Record team.

A.2.3. Review of access audit results is a shared responsibility between the YCHHS HIPAA Privacy Officer, Administrative Services Director and/or designees.

B. Access Establishment and Modification:

B.1. YCHHS will review the access privileges assigned to workforce members at least annually or when there is a change to an individual's duties and responsibilities (See the *YCHHS Professional Development Plan and Performance Appraisal*).

7. SECURITY AWARENESS AND TRAINING

A. Training:

A.1. See YCHHS policy # 016-79-04-32, *Mandatory Training and Tracking Requirements.*

B. Security Reminders:

B.1. The YCHHS HIPAA Privacy Officer, Administrative Services Division, and the Yamhill County Information Technology Division will collaborate to send out security alerts,

advisories, and directives of security-related information to those workforce members and other entities as applicable.

C. Protection from Malicious Software:

C.1. Installation of software to all Yamhill County computing devices will comply with the Yamhill County policy *Employee Use of County Computers*.

C.2. YCHHS security awareness training will include information pertaining to protection from malicious software.

D. Log-in Monitoring:

D.1. Track and document system security incidents:
Current process is to document internally to Yamhill County IT via email. A policy in the development process will specify a security incident logging scheme to track such events. One recent example is a threat stemming from an employee of a partner agency who had their system compromised, resulting in a malicious attachment to entries from their address book. Yamhill County IT sent an e-mail alert to all county workforce immediately explaining the nature and severity of the threat.

D.2. Maintain records of incidents:
The completed security incident policy will require a log of all security incidents that:

D.2.1. Specifies the origin and nature of the threat;

D.2.2. Provides an explanation of how the threat was identified;

D.2.3. Documents how the Yamhill County IT team reacted, including what software or techniques were used; and

D.2.4. Documents the final disposition of the security incident episode, including any damaged systems, corrupted files and the staff time required to deal with the event.

D.3. Evaluate incidents for trends and how they were handled:
The security incident log maintained by Yamhill County IT will allow review over time of trends and will spotlight improvements in how such threats are identified, reacted to, and resolved.

D.4. Automated mechanisms for tracking security incidents and collecting/analyzing incident information:
There is no automation at this time related to security incidents and analyzing an event except for:

D.4.1. The Bit-Defender or Untangle programs that run on the network at all times can and do automatically and actively block identified threats. Such events require no staff interaction, although the protection is only as good as the current signature files in place that indicate the "fingerprint" of a malicious threat.

D.4.2. The firewall actively blocks hacking attacks that originate from the public switched network known as the internet. No Yamhill County IT staff interaction is required, and the firewall software logs the unauthorized intrusion attempts that fail to breach the firewall.

E. Password Management:

E.1. See YCHHS policy #016-79-09-10, *Technical Safeguards* section, 4. Unique User Identification.

E.2. The Yamhill County and YCHHS EHR policy is for all system users to keep their passwords confidential. Initial passwords are provided with a one-time logon, requiring a user to set their password to something only they know.

E.3. The EHR system is configurable in terms of setting:

E.3.1. The number of unsuccessful password attempts before the user account is disabled;

E.3.2. The relative "strength" of a password required when resetting a password;

E.3.3. The minimum password length;

E.3.4. The number of days that a password is valid before it needs to be reset;

E.3.5. The length of time that a user will be able to reconnect to a session that terminated.

E.4. Current settings include a requirement for strong passwords, a 90-day password life cycle and five incorrect logon attempts before a user account is disabled:

E.4.1. The network management by Yamhill County IT of the Active Directory system requires a strong password to be reset every 90 days.

E.5. Portable devices and data security, including laptops, notebook tablets, smart phones – See YCHHS policy #016-79-05-01, *Mobile Computing Device Security Policy.*

8. SECURITY INCIDENT PROCEDURES

A. Response to Security Incidents:

A.1. Incident response procedures for all YCHHS workforce members are included in the YCHHS annual HIPAA Security and Awareness Training

A.2. In addition to the annual HIPAA Security and Awareness Training, YCHHS supports annual professional training for its eligible employees related to the individual's roles and responsibilities.

A.2.1. See YCHHS policy #016-79-04-04, *Employee Continuing Education, Training and Professional Development*

A.3. Incident Response Testing:

A.3.1. YCHHS shares management of the Juniper production server with Yamhill County IT. YCHHS is responsible for database management and assuring that file system entries related to the Juniper environment and the MySQL database are copied to the backup platform. On a daily basis the database is fully backed up, the file system changed entries copied to the secondary platform, the database backup "dump file" is copied to the secondary server, and a scheduled process restores the database on the secondary server. That is essentially testing

each day that the database and file system restore processes result in a live copy of the EHR production environment that is operational. This process does not complete when there is any corruption of a database object or an indication in the "MySQL" scheme database.

A.3.2. The YCHHS policy #016-79-05-06, *Electronic Health Record System Backup and Recovery Process* functions as the "checklist" to use in the event that the database does not properly back up. The checklist is used for cloning the database and restoring it. The internal validation of the database when creating a dump file fails at any errors, which can be as simple as a query that references a field that has been renamed or removed. In those situations where there is a database issue, the Juniper server will be reviewed for log files indicating the exact nature of the error.

A.3.3. Automated mechanism to test the incident response capability?
Neither Yamhill County IT nor the EHR currently have an automated mechanism related to capturing incidents or tracking the related events and disposition.

A.4. YCHHS HIPAA Privacy Officer will collaborate with the YCHHS Administrative Services and/or Yamhill County Information Technology Division as applicable to address incidents involving information systems.

A.4.1. The YCHHS Administrative Services Director or designee is responsible for researching any claim that something improper had happened within the EHR system. Confirmation that a particular workforce member viewed restricted records or that the audit log documented a particular event would be provided to YCHHS Administration.

A.4.2. YCHHS HIPAA Privacy Officer and/or YCHHS Administration would then be responsible for determining whether such access failed to meet the "need to know" standard or violated confidentiality policies in some way. If in the judgement of YCHHS Administration the access violated internal policy or regulatory requirements, a workforce member could experience consequences up to and including termination of employment (See policy #016-79-09-11, *Enforcement, Sanctions, and Penalties for Violations of Individual Privacy*).

A.5. Continuity of Operations: See YCHHS Administrative Services and Yamhill County Information Technology Division Continuity of Operations Plan (COOP).

B. Security Incident Reporting:

B.1. Incident Response Reporting – YCHHS workforce will report suspected security incidents to the YCHHS HIPAA Privacy Officer;

B.2. YCHHS HIPAA Privacy Officer logs all reported incidents in the YCHHS HIPAA Incident Log;

B.3. YCHHS HIPAA Privacy Officer reviews each incident, takes the appropriate action, and records the decision rendered and action taken.

9. CONTINGENCY PLAN

A. Data Backup and Disaster Recovery Plan:

A.1. See YCHHS policy # 016-79-05-06, *Electronic Health Record System Backup and Recovery Process*.

B. Emergency Mode Operation Plan:

B.1. See YCHHS Administrative Services and Yamhill County Information Technology Division COOP plans

C. Testing and Revision Procedures:
The primary goal of the contingency plan is to assure that the production system can quickly recover from any unforeseen hardware or software issues and be made available to the user community after the shortest possible delay.

Currently the revisions in scheme involve an off-site server at the City of McMinnville data center located at the police station. The same backup process used internally will be set up on a true copy of the hardware component in the Yamhill server room located at that site. It will be the same as the current in-house backup server in technique but locating the backup offsite is a major improvement in compliance with suggested backup architecture. Once the parallel backup server is operational and it is confirmed that a previous day copy of the Juniper server is accessible and operational, the revision in procedures will be set up. The idea is to "re-play" log files periodically. That is, a history table in the MySQL database describes each event in exacting detail – that event could then be replicated on the copy of the production server located offsite. That would likely reduce the latency of the backup server from 24 hours to approximately 30 minutes.

10. PERIODIC TECHNICAL AND NONTECHNICAL EVALUATION

A. Physical Access Monitoring:

A.1. Monitors physical access to the facility where the information system resides to detect and respond to physical incidents. This includes:

A.1.1. Access outside normal work hours:
All county offices where the EHR system is used have electronic access control systems. Each workforce member is assigned appropriate levels of access to particular buildings during particular days and times of the week. For workforce members needing after-hours access, their electronic access is configured to support entry to buildings during those times.

A.1.2. Repeated access to areas not normally accessed:
It is possible to use the electronic access control to track over time what is "typical" access for a workforce member. The workforce member can then compare this data against a typical profile of access usage.

A.1.3. Accesses for unusual lengths of time:
The YCHHS EHR team is able to generate a report regarding the length of an EHR session and the activity during the session. If a workforce member leaves an EMR record open during the overnight, it will appear that they are on the system since the previous day due to the automatic session termination not killing a session that has an open and unsaved record.

A.1.4. Out-of-sequence accesses:
Out of Sequence access implies a data mining operation is in effect that will identify what is "normal" for a particular user and then identify out of normal range activity. That could be someone coming into the office at night when they normally work an 8 to 5 shift. Monitoring occurs via retrospective review of data log reports activity.

A.2. Reviews access logs:
Review of access logs is not structured, but rather done at a particular interval or part of a typical system administrator day. The logs are reviewed on a regular basis primarily to determine that all relevant data is being captured and that the log rotations are happening as scheduled. These logs can also be used to review and analyze access behavior suggesting violation of access protocols.

A.3. Coordinates results of reviews and investigations with the YCHHS organizational incident response capability:
The YCHHS HIPAA Privacy Officer and the YCHHS Administrative Services Director coordinate as applicable with the YCHHS EHR team, Yamhill County IT Manager, Yamhill County Administration, and YCHHS managers to develop a plan of action to address findings from the investigation and mitigate further incidences.

B. Information System Monitoring:

B.1. Monitors to detect:

B.1.1. Attacks and indicators of potential attacks:
Yamhill County IT has several layers of intrusion detection and prevention of unauthorized or malicious access. That includes a Palo Alto Firewall, in addition to Bit Defender and Untangle software.

B.1.2. Unauthorized local, network, and remote connections:

Yamhill County IT manages all network and remote connections.

B.2. Identifies unauthorized use of the information system through:

B.2.1. The front end of system access, requires using a personally identifiable logon which has a set of user rights applied to it that is reflective of what a workforce member requires to perform their job duties. Every effort is made to fine tune group profiles which generally drive system access so that only the necessary access rights are applied.

B.2.2. Unauthorized use of the EHR can mean many different things:

a) If the logged in user is who they claim, typical user rights restrictions and limitations on functionality limit what can done. Unauthorized access may or may not be immediately identified. Forensic review of such things as "client access" or "restricted client access" can sometimes spotlight access-requiring justification to support.

1) On "restricted clients", there is an expectation that a valid reason will be provided by the user for each access of a restricted client record per day.

b) If the logged in user is NOT who they claim to be, such as in the case of logon

credential security being compromised, there is no live monitoring that would prove who is logged in at that time is not the genuine owner of the logon credentials. Recognizing that type of misrepresentation cannot be done in real time, but rather requires a retrospective review and investigation as outlined above.

B.3. Deploys monitoring devices:
Yamhill County IT deploys real-time monitoring devices related to anti-virus and anti-malware threats. Internal to the EHR system, there is a reliance on retrospective review and analysis of data, such as:

B.3.1. Strategically within the information system to collect organization-determined essential information primarily involving database integrity and verification that all overnight processes are completed properly; and

B.3.2. At ad-hoc locations within the system to track specific types of transactions of interest to the organization such as with the State Measures and Outcomes Tracking System data related to clients in treatment, crisis services, involuntary services, and episode-ending service conclusions.

B.4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion:
Yamhill County IT is responsible for all intrusion-monitoring devices and tools, including configuration, version, and capability to review logs of activity. Information collected is stored in a secure folder with access permission granted by the Yamhill County IT Manager.

11. BUSINESS ASSOCIATE CONTRACTS/QUALIFIED SERVICE ORGANIZATION AGREEMENTS AND OTHER ARRANGEMENTS

A. See Policy #016-79-09-07, *Business Associate Relations and Qualified Service Organizations*

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Physical Safeguards 45 CFR §164.310

POLICY NUMBER: 016-79-09-09

Table of Contents

1. PURPOSE

It is the policy of YCHHS that all personnel preserve the integrity and confidentiality of health and other sensitive information pertaining to Yamhill County clients. The purpose of this policy is to ensure that YCHHS has systems, policies, and procedures to limit physical access to its protected health information and the facilities in which they are housed, while ensuring that those with proper authorization have the necessary required access.

2. TERMS

- **Physical Safeguards:** Are physical measures, policies, and procedures to protect a covered entity's or business associate's protected health information and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion (§164.304).

- **Role Based Access:** Is access control based on users' role. It is a form of security allowing access to protected health information based on job function allowing workforce access only to the minimum necessary information to fulfill their job functions. A given role may apply to a single individual, several individuals or to a team.

- **Sanitization**: Is the process to remove information from media prior to disposal or reuse, such that data recovery is not possible. Examples include media found on scanners, copiers, printers, desktop computers, laptops, notebook computers, and mobile devices. It includes removing all classified labels, markings, and activity logs.

3. GENERAL PROCEDURES

A. **General:**

A.1. YCHHS must take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information.

B. **Facility Access Controls:** YCHHS will work closely with Yamhill County Facility Maintenance and Yamhill County Information Technology Departments to ensure as reasonably possible that YCHHS client health information is stored in a secure location and the integrity of that information is protected from natural and environmental hazards, and unauthorized intrusions.

B.1. Contingency operations – See YCHHS *Continuity of Operations Plan* (COOP) for details.

B.2. Facility Security – YCHHS Workplace Practices:

B.2.1. YCHHS client protected health information will be stored in secure locations requiring use of a key or electronic key card to access the information stored in paper or electronic format by authorized individuals.

a) See Yamhill County policies:

1) Courthouse Security and Access Policy

2) Courthouse Keys Policy

b) Yamhill County's Facility Maintenance Department, Information Technology and/or YCHHS, will maintain a log of all keys and/or electronic key cards issued to authorized individuals.

c) All access to secure locations using an electronic key card will be logged, monitored, and maintained by Yamhill County's Information Technology Division. Logs are available to YCHHS Administration for review upon request.

B.2.2. Authorized Yamhill County workforce will be issued an ID badge/electronic key card to assist with validation of authorized access to secure locations.

B.2.3. Visitors with access to secure locations where health information is stored will (§164.310(a)(2)(iii):

a) Sign a visitor access record to include: name, organization of person visiting, visitor's signature, date of access, entry and departure times and purpose of visit; and

b) Be accompanied and monitored as reasonably possible by authorized individual.

B.2.4. Lost keys or electronic key cards to YCHHS facilities:

a) YCHHS workforce will report any lost keys or key cards to supervisor;

b) Yamhill County Information Technology Division will disable lost key cards;

c) Yamhill County Facility Maintenance will change locks to secure locations if determined there is a high risk that the security of the facility is compromised.

B.3. Role Based Access:

B.3.1. See policy #016-79-09-06, *Minimum Necessary Information*, Section 5. *Access and Uses of Information.*

B.4. Additional YCHHS Workplace Practices:

B.4.1. Paper:

a) Each YCHHS workplace will store files and documents in locked rooms or storage systems.

b) In workplaces where lockable storage is not available, YCHHS staff must make reasonable efforts to ensure the safeguarding of confidential information. At a minimum, records should:

1) Preferably be behind two locked doors, or

2) In a locked room, or

3) Constantly monitored during business hours by YCHHS staff to prevent unauthorized access.

c) Each YCHHS workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.

d) Each YCHHS workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

B.4.2. Oral:

a) YCHHS staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.

b) Each YCHHS workplace shall make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.

1) **Exception:** In work environments structured with few offices or closed rooms, such as open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that YCHHS has met the reasonable safeguards and minimum necessary requirements.

c) Locations of verbal exchange with various risk levels:

1) Low risk: Interview rooms, enclosed offices, and conference rooms.

2) Medium risk: Employee only areas, telephone, and individual cubicles.

3) High risk: Public areas, reception areas and shared cubicles housing multiple staff where clients are routinely present.

B.4.3. Visual:

a) YCHHS staff must take reasonable efforts that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.

b) Computer screens: Each YCHHS workplace must make a reasonably good faith effort to ensure that confidential information on computer screens is not visible to unauthorized persons. Suggested means for ensuring this protection include:

1) Use of polarized screens or other computer screen overlay devices that shield information on the screen from persons not the authorized user;

2) Placement of computers out of the visual range of persons other than the authorized user;

3) Clearing information from the screen when not actually being used;

4) Locking-down computer workstations when not in use;

5) Utilize password-protected screensaver; and

6) Other effective means as available.

c) Paper documents: YCHHS staff must be aware of the risks regarding how paper documents are used and handled and must take all necessary precautions to safeguard confidential information.

B.4.4. YCHHS staff must take special care to ensure the protection and safeguarding of, and the minimum necessary access to, paper and electronic documents containing confidential information that are located on:

a) Desks;

b) Fax machines;

c) Photocopy machines;

d) Portable electronic devices (e.g., cell or smart phones, laptop computers, travel drives, etc.);

e) Computer printers; and

f) Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

C. **Transportation of Media Containing Protected Health Information (includes diskettes, flash drives, compact disks, paper, and microfilm):**

C.1. Only authorized workforce members or those individuals or organizations authorized by YCHHS administration shall transport media containing health information outside the secure controlled area.

C.2. Access agreements will be used for non-YCHHS workforce transporting protected health information to document individual's responsibility to safeguard PHI as follows:

C.2.1. Business Associate agreements.

C.2.2. Contractor agreements.

C.3. Paper records and unencrypted or non-password protected electronic media - When transporting paper documents or unprotected electronic media containing PHI, YCHHS staff must follow the expectations below:

C.3.1. PHI must be transported in a closed and locked device such as a bag or box. Bags with locks will be provided to staff who need them to perform the functions of their job.

C.4. Electronic portable devices such as phones, laptops, and tablets shall not be left unattended for any length of time and shall remain with the employee at all times when off site.

C.4.1. See YCHHS policy # 016-79-05-01, *Mobile Computing Device Security Policy.*

C.5. Flash/USB/Thumb Drive – Protected health information saved to a USB drive that will be transported outside a secure location should be saved to a password protected flash drive such as the Iron Key USB Flash Drive, otherwise will need to be transported as directed above under C.3.1.

D. **Disposal of Electronic Health Information and Sanitization of Devices Containing Protected Health Information:**

D.1. Yamhill County Information Technology Division is responsible for sanitizing electronic computing devices prior to disposal or reuse.

D.2. The YCHHS designated Administrative Services staff will be responsible for sanitizing cell phones prior to disposal or reuse.

D.3. YCHHS Departments are responsible to ensure copiers, scanners, and printers capable of storing protected health information will be sanitized prior to removal from a YCHHS facility for servicing or disposal.

D.4. **Behavioral Health Only:** When an SUD client sends an incidental message to the personal device of an employee of a Part 2 program, the employee will be able to fulfill the Part 2 requirement for "sanitizing" the device by deleting that message. (§2.16(a)(2)(ii); *Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule,* July 13, 2020)

E. **Record of the Movements of Hardware and Electronic Media (§164.310(d)(2)(iii):**

E.1. Yamhill County Information Technology Department is responsible for maintaining record of desktop computers, laptops, computer notebooks and tablets assigned to YCHHS workforce.

E.2. YCHHS Administrative Services designated staff is responsible for maintaining record of smartphones assigned to YCHHS workforce members.

E.3. YCHHS Office Manager and/or designee is responsible to ensure copiers and fax machines that store PHI are sanitized prior to removal from YCHHS secure locations.

E.4. YCHHS workforce using electronic media such as thumb drives, CD-ROMs, and audio/video recordings are responsible to ensure the media is stored in a secure location and all PHI stored on the media is removed prior to the electronic media's disposal.

E.5. Yamhill County IT utilizes IBM MaaS360 to locate lost or stolen YCHHS issued cell phones. In addition, IBM MaaS360 can be used to wipe a phone remotely and clear the passcode to ensure PHI stored on YCHHS issued cell phones is protected.

F. **Access Agreements for Non-workforce Members or Business Associates:**

F.1. YCHHS will utilize access agreements for those individuals, organizations, and/or agencies that are not part of the workforce, or a business associate, that require access to YCHHS client protected health information. Agreements will be maintained on file as required by record retention laws.

F.2. **Behavioral Health Only**: Audit and evaluation activities performed by government agency or private person which provides financial assistance to YCHHS for substance use treatment or authorized by law to regulate YCHHS substance use treatment activity or determined by the YCHHS program director or designee to be qualified to conduct the audit or evaluation activities (42 CFR Part 2, §2.53).

F.2.1. Records not copied or removed: Person agrees in writing to comply with the limitations on redisclosure.

F.2.2. Records copied or removed from secure controlled area: Person agrees in writing to:

a) Maintain the patient identifying information in accordance with requirements in 42 CFR Part 2, §2.16;

b) Destroy all patient identifying information upon completion of the audit or evaluation;

c) Retain records in compliance with applicable federal, state, and local record retention laws;

d) Comply with limitations on redisclosure; and

Except as provided in paragraph (e) of section §2.53, patient identifying information disclosed under this section may be disclosed only back to the part 2 program or other lawful holder from which it was obtained and may be used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by a court order entered under §2.66.

G. **Electronic Health Record Data Backup and Storage:**

G.1. Yamhill County information Technology is responsible for maintenance and repair on the information system components and hardware used for the storing of YCHHS electronic client protected health information.

G.2. Electronic Health Record Backup:

G.2.1. See YCHHS policy # 016-79-05-06, *Electronic Health Record System Backup and Recovery Process.*

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Technical Safeguards 45 CFR §164.312

POLICY NUMBER: 016-79-09-10

Table of Contents

1. PURPOSE

It is the policy of YCHHS that all personnel preserve the integrity and confidentiality of health and other sensitive information pertaining to Yamhill County clients. The purpose of this policy is to ensure that YCHHS has the systems, policies, and procedures in place to assure that only those persons authorized have access to the information systems that maintain electronic protected health information.

2. TERMS

- **Encryption** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **HTTPS** consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer.
- **Raintree** is the Electronic Health Record software application YCHHS has named Juniper.
- **SFTP** means Secure File Transfer Protocol (also known as SSH File Transfer Protocol) is a network protocol that provides file access, file transfer, and file management over any reliable data stream.
- **Technical Safeguards** means the technology, and the policy and procedures for its use that protect electronic protected health information and control access to it. (§164.304)
- **VPN** is a Virtual Private Network that is a virtualized extension of a private network across a public network, such as the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

3. GENERAL PROCEDURES

A. YCHHS will:

A.1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (PHI) it receives, maintains, or transmits.

A.1.1. Electronic Health Record (i.e., Juniper): Communication between the Juniper server and a Juniper client program, even if run from a remote location, is encrypted end to end.

A.1.2. Remote Desktop: For staff that use the "remote desktop" system to log in and run a Juniper session from an in-house server, the traffic is encrypted end to end regardless the location of the remote user because the remote desktop program manages the connection between the client computer and the server.

A.1.3. Electronic PHI Availability: Every effort is made to keep the system available almost around the clock. The system will be unavailable for 15 minutes early every morning when a dump file is generated to supply to the backup server, which is required to synch the back-up server with production. A few of the overnight hours include some intensive derived dataset construction operations which don't technically lock users out but which could make system navigation sluggish and introduce significant delays; primarily between midnight and 2am.

A.2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. Protection mechanisms fall into both "hardware" and "administration" categories.

A.2.1. To address hardware vulnerabilities, one key aspect is redundancy. This includes such things as having two mirrored C drive partitions that run the operating system on a critical server system. If one of the hard drives were to fail, the system switches to the second one automatically to avoid any down time.

A.2.2. Backups of production are monitored daily. The entire database is output through a standard MySQL process and re-loaded minutes later on a secondary server. File system entries outside the database are copied overusing a secondary file synchronization process.

A.2.3. Not only are timely back-ups critical, but also the strategies to recover from hardware or database failure. For example, we may have a backup that is fully restored on a backup server but is 5 hours old. To recover data to current, it is necessary to restore the earlier dump file, and then run the log entries created after the dump file was output to catch up the copy of the production database to current.

a) System Development Note: A Yamhill County IT project is underway to configure a fully mirrored database system where file system changes are copied over frequently, and database changes are updated by running log files on the "slave" server to run the same updates that happened manually by end users in production.

A.2.4. Alerts are monitored by the Yamhill County IT department relative to server systems to identify situations. As an example, a backup server indicated errors on a memory slot; requiring a system board replacement because of a faulty memory slot on the system board. Without the alert and action taken by County IT system administrators, a hardware failure could have resulted. Proactive protective mechanisms due to "administrative" processes such as the above help to guard against sudden and unexpected failures.

A.3. Protect against any reasonably anticipated uses or disclosures that are not permitted or required by HIPAA.

A.3.1. Staff training is the key to avoid HIPAA violations. Each workforce member is required to receive training at hire, then annually thereafter and as needed, to review data security rules and acknowledge that they understand the HIPAA fundamentals, such as using secure email when PHI is involved in any correspondence going outside the local domain (see policy #016-79-04-32, *Mandatory Training and Tracking Requirements*).

A.3.2. All disclosures made outside the YCHHS organization shall be accompanied by specific instructions not to re-disclose and to destroy records if the receiving party is not the intended recipient of the protected health information. E-mail and fax transmission footers contain various disclosure statements and re-disclosure prohibitions.

A.4. Ensure compliance by all workforce members.

A.4.1. All YCHHS workforce members are required to review HIPAA compliance and data security guidelines at hire, annually thereafter and as needed.

A.4.2. Computer sessions are automatically locked after 15 minutes of idle time for all users in the YCHHS group in order to protect against people leaving their sessions up when they are away from their workstation.

A.4.3. Network rights limit visibility of network file volumes to exclude areas where the staff member is not directly involved. Network rights are approved by YCHHS supervisors and access permissions created by Yamhill County IT.

4. UNIQUE USER IDENTIFICATION

A. Identification and authentication of YCHHS information system users

A.1. YCHHS workforce is required to use strong password to:

A.1.1. Log-on to County owned computing device, access County Network and personal smart phones used for YCHHS business.

a) Yamhill County Information Technology requires passwords be updated every 90 days

b) See Yamhill County document, *Creating a* "Strong Password" located on the HHS Intranet under Technology Support

c) See YCHHS policy #016-79-05-01, *Mobile Computing Device Security Policy*

d) See *YCHHS Cell Phone Agreement*

A.1.2. Access workforce member's County voicemail system:
The digital voice mail system has a specific user associated with any voice mail inbox and all are password protected. Network administrators can reset those passwords as needed if someone forgets their password or leaves the organization without reviewing voice mail entries.

A.1.3. Remote Desktop:
Remote Desktop access is provided on a case-by-case basis for workforce members who require access from off-site locations. The transmissions related to remote desktop access are encrypted end to end where the traffic travels outside of the county domain.

A.1.4. YCHHS information system accounts, including:

a) Electronic Health Record: All access requires a personally identifiable logon.

b) Ahlers Clinical Visit Record; ALERT Immunization Information System (ALERT IIS); Clinical Integration Manager (CIM); E-Prescribing Software; Express Payment & Reporting System (eXPRS); Medicaid Management Information System (MMIS); and One Health Port: Each workforce member with access to these systems has a personal logon account managed by the system administrator.

c) Oregon Record Management System (ORMS): Workforce members are assigned a secure logon and password to look up scanned documents that are uploaded to the document management repository in Baker City, Oregon. The transmission of documents to ORMS or searching for documents via the ORMS interface happens on an encrypted channel.

B. YCHHS electronic health record system uniquely identifies and authenticates organizational users. YCHHS will assign a unique name and/or number for identifying and tracking users of the electronic health record.

B.1. Manage individual identifiers:

B.1.1. Individual(s) authorized to assign identifier:
The Electronic Health Record support team creates user account records.

B.1.2. Selecting the identifier:
Typically the "system ID" for a workforce member is their employee number, although contractors are set up using their initials.

B.1.3. Assigning the identifier:
same as above

B.1.4. Preventing reuse of identifiers:
There is no reuse of system ID's representing a user account – when someone leaves the organization their account is "disabled" to prevent potential re-use and left as a disabled account so that any future audits can link historical database activity with the name of who was logged in at the time.

B.1.5. Disabling the identifier after period of inactivity:
A user account will only be disabled if the workforce member leaves the organization. There are accounts set up for some managers, for example, that are seldom used, but for which access must be retained in spite of unpredictable login frequency.

C. Virtual Private Networks (VPN) access:
VPNs are set up with very specific criteria – any VPN connection used to access the Yamhill County system is limited by the origination IP address. That address is embedded in the firewall setup to support the VPN connection. It is not just a logon name and password, but also the source address of the connection request that is validated at the front end prior to allowing access via the VPN. These VPN logons are active directory user accounts, so can be managed in the same way that Yamhill County IT manages accounts for the typical workforce member. For VPN access, there is an extra hook due to usage of a VPN software package called *GlobalProtect*.

5. EMERGENCY ACCESS PROCEDURE

A. **See *YCHHS Continuity of Care Plan:***

A.1. If the EHR system is unavailable due to a system failure of some kind, a power outage, a database issue, a production system server issue or a network issue, or a

major catastrophic event, Yamhill County IT and Electronic Health Record support staff have backup processes to employ.

A.2. The EHR support team will focus on the system recovery required to get the system operational. That could involve database objects, vendor code, virtual server issues, network issues, server computer software issues, or hardware issues involving key server components. In many potential downside scenarios, Yamhill County IT is a key player in diagnosis and recovery. Where the issue is self-contained, such as a key data table in the production database becoming corrupted, the EHR support team would address the issue with little or no involvement from County IT. In the event of a "system down" event, the contractor for the EHR system would also be contacted immediately for assistance to triage and remedy the issue.

B. See YCHHS policy # 016-79-05-06, *Electronic Health Record System Backup and Recovery Process.*

C. Contingency plan for information systems:

C.1. Essential missions and business functions:

C.1.1. See *YCHHS Continuity of Care Plan.*

C.2. Recovery objectives, restoration priorities and metrics:

The primary EHR system consists of database objects, disk resident file objects (forms, lists, scripts), and several compiled executable components. The database objects include the production database itself and the companion MySQL database, which contains all the user rights and database schema.

All those pieces need to be in synchronization with each other since the compiled components evaluate table definitions through "EMR plug-ins" and the database objects need to agree with the definition. If not, the compiled component of the system will automatically fire changes to get those components in synch.

The key restoration priority is to achieve a business-as-usual status for YCHHS support staff functioning normally. That will always be the goal of any recovery or remediation scenario. This implies the EHR support team will prioritize restoration of basic functionality and system availability above all else. Second priority will be restoration of the clinical electronic medical records.

The metrics to indicate success is that most of the user community can do their day-to-day work in an operationally sound computing environment without excessive delays or malfunctions.

C.3. Assigned contingency roles and responsibilities with contact information:

C.3.1. See YCHHS policy # 016-79-05-06, *Electronic Health Record System Backup and Recovery Process*.

C.3.2. The EHR support team emergency contact information and assigned roles is available upon request from the YCHHS Administrative Services Director and/or designee.

C.4. Maintaining essential missions and business functions despite Information System disruption, compromise, or failure:

The key to maintaining business functions is the availability of alternative information sources and processes so that staff can operate to serve clients even if the EHR system is temporarily unavailable. This will include workarounds such as writing a service note on paper, or any number of normal EHR tasks without the EHR being available. With some documents no longer added to the client paper chart, supervisors are responsible to assure that at least a minimal baseline of operations is possible if there is an extended disruption in EHR system availability.

C.5. Eventual, full information system restoration without deterioration of the security safeguards. In the event that the system does have a major failure of some sort, to assure that the security safeguards and audit trail are in place, the EHR support team will:

C.5.1. Identify the status that existed after a failure of some kind was noted

C.5.2. Understand how to potentially reload an earlier copy of the database via backup/restore, and then "replay" log files to fire the same edits that had been done on the system from the time the backup being restored was generated.

C.5.3. Review the status of the system for operational usage after a baseline is re-established for re-starting the system.

6. ELECTRONIC HEALTH RECORD AUTOMATIC LOGOFF

A. Session lock:
Juniper sessions lock automatically if there is 30 minutes of inactivity on a session and requires re-entering the password to unlock it.

B. Session termination:
Sessions are terminated after two hours of inactivity unless there is an unsaved record in their session. Under that condition, the session stays locked, but is not terminated.

7. ENCRYPTION AND DECRYPTION OF ELECTRONIC PROTECTED HEALTH INFORMATION

The "local" Juniper client program uplinks to the Juniper server on an encrypted channel as designed by the vendor. If the connection is first to a remote desktop server, that uplink channel is also encrypted end to end via Windows Remote Desktop software.

8. AUDIT CONTROLS

A. **Access Controls:**

A.1. YCHHS Workforce members are trained per the YCHHS Role-Based Access Protocol and Criteria and the minimum necessary standards.

Workforce members are aware that record access is tracked and providing justification for reviewing certain clinical records could be required. Unauthorized or unnecessary review of clinical records is forbidden via policy.

A.2. The electronic health record platform allows the organization to control which workforce members have access to the data of specific clients. This includes the client's files, appointment-related information, and ledger items. The EHR access control has three basic access parameters:

A.2.1. Everyone: Access to the patient's data is granted to all users, except users that are restricted from this patient's files.

A.2.2. "Break the Glass": Upon accessing the patient's data, you are prompted to provide a reason for doing it. Every such access request is logged and displayed in a history list.

A.2.3. Limited to ACL Only: The patient's data is accessible only to the users who have been granted access to it through the Access Control List or have been allowed to "break the glass".

B. **Additional Access Controls:**

B.1. Password changes: Required every 90 days, with limits on re-using previous passwords and requirements for strong passwords are enforced by active directory.

B.2. Failed logons: Automatic locking of a user account after three incorrect logon attempts.

B.3. Admin privilege usage: A small number of database accounts approved by the YCHHS Administrative Services Director are set up with administrative rights that allow for operations that require create, delete, truncate and execute access rights.

B.3.1. VPN access:
Only the EHR vendor and the Raintree consultant log in through a VPN and have privileges to the database. That is necessary for ongoing support.

C. **Log events and maintain record:**

C.1. What type of event occurred:

C.1.1. History table: Action indicates update, insert or delete.

C.1.2. Audit log table: The Audit Log table is a Juniper construct to track HIPAA related events. The type of event may be listed as "Action=Showing Patient List" and a search key value of the patient ID that had been searched.

C.2. When the event occurred:

C.2.1. History table: Each history log entry has a timestamp down to the millisecond.

C.2.2. Audit log table: Has UNC Time Stamp field.

C.3. Where the event occurred:

C.3.1. History table: Notes "Local Area Network ID" where event occurred and the user account logged in.

C.3.2. Audit log table: Displays network access point ID that indicates the IP address of the workstation from where the Raintree logon originated.

C.4. The source of the event:

C.4.1. History table: Notes "Local Area Network ID" where event occurred and the user account logged in.

C.4.2. Audit log table: User ID and User Name (RT logon) are both listed in each record.

C.5. The outcome of the event:

C.5.1. History table: The History table does not show an explicit outcome – it lists the type of event and the "values" associated. For example, on an appointment related entry it would indicate insert of a new entry, and the "values" column would show what the various data elements were such as date=, time=, doc=, etc.

C.5.2. Audit log table: The Audit Log is focused on what someone had access to, not whether they did a particular thing once they opened the record.

C.6. Identity of any individuals or subjects associated with the event:

C.6.1. Juniper logs all the events that relate to records being viewed, added, changed, or deleted. That includes all the C1-C6 metrics. Those logs are rotated from database table to disk archive on a routine and timed basis via a Juniper secondary service focused on log rotation and related database operations.

C.6.2. These logs only reflect activity that happened internal to database operations.

D. **Audit Report:**

All aspects of system usage are tracked and can be reported against. The extraction of the data requires specific querying by system administrators. It is possible to consolidate the Raintree logs into a more powerful searchable repository to accomplish better end user report-ability of system access and activity. To the extent that any particular system events can be traced back to the origin of any edits, the system can be fully audited.

9. PROTECTION OF ELECTRONIC HEALTH INFORMATION FROM IMPROPER ALTERATION OR DESTRUCTION

A. Record Destruction: Each YCHHS program adheres to the archive/retention rules established by the Oregon Secretary of State. Whenever a client re-opens for services, the destruction of records countdown starts over.

B. Improper Alterations Safeguards:

a. First line of defense against improper alterations and/or destruction of the record is staff training as stated above in Section 3.A.3.1.

b. The second line of defense is the user access rights outlined above in Section 3. General Procedures and Section 4. Unique User Identification. These access rules confine users to activities they are authorized to perform, and validation logic keeps the business rules firing properly and guards against unauthorized access to the database and servers.

c. Lastly, the EHR audit and reporting capabilities identified under section 8 above provides YCHHS the ability to perform retrospective reviews of data to identify improper alterations or destruction of the record, e.g., anomalies, discrepancies and activity that is outside the norm, such as a provider from a

non-behavioral health program area modifying a behavioral health record.

10. MECHANISMS TO VERIFY THAT ELECTRONIC PROTECTED HEALTH INFORMATION HAS NOT BEEN ALTERED OR DESTROYED IN AN UNAUTHORIZED MANNER

Any data transferred to or from servers at the data center is analyzed by standard and typical check-sums and other internal calculations to assure that what was sent is the same as what was received.

11. CONTROLS TO VERIFY THAT A PERSON OR ENTITY SEEKING ACCESS TO ELECTRONIC HEALTH INFORMATION IS THE ONE CLAIMED

A. **Unique user ID**:
It is a violation of county policy to share user accounts, share passwords, or otherwise interfere with the ability to determine the staff member that was responsible for any particular system setting or database modification. Each staff member has a unique user ID that is used by only them.

B. **Non-organizational users**:
Users outside the organization may or may not have a logon to the EHR. Various partner agencies have accounts as authorized by HHS Administration for the purpose of care continuity and case management assistance. Those accounts are under the same framework as internal staff.

12. TRANSMISSION SECURITY TO GUARD AGAINST UNAUTHORIZED ACCESS TO INFORMATION TRANSMITTED OVER AN ELECTRONIC COMMUNICATIONS NETWORK

A. Yamhill County Information Technology Division is responsible for implementing and maintaining an information system that reasonably protects the confidentiality of protected health information transmitted via secure email when appropriately used by the workforce.

If client PHI is sent via e-mail to another domain, so that the traffic is routed on the public switched network, staff are required to use "secure e-mail". That means that the recipient of the e-mail only gets a link to the information. The content to be sent is stored internally and the link the other party receives is used to access the information over a secure HTTPS connection. This avoids sending out PHI on an unencrypted link.

B. See YCHHS policy # 016-79-03-02, *Electronic Communication With or About Clients*.

13. INTEGRITY CONTROLS TO ENSURE THAT ELECTRONICALLY TRANSMITTED INFORMATION IS NOT IMPROPERLY MODIFIED WITHOUT DETECTION UNTIL DISPOSED OF

Any "improper modification" of electronically submitted data would be identified and flagged by a program that manages the transmission of data. That would be due to using "check sums" and other low-level authentication processes, whether that is on an

email server or an SFTP server or a remote desktop server. The transmission fails with an error if the packets received do not match the hash key supplied with a packet.

14. ENCRYPTION MECHANISM TO ENCRYPT ELECTRONIC PROTECTED HEALTH INFORMATION WHENEVER DEEMED APPROPRIATE

Encryption is only necessary when traffic related to PHI data is sent outside the Yamhill County domain. Internal network switching does not encrypt and de-encrypt traffic on the fly. See the following sections of this policy for additional information regarding encryption:

3. General Procedures

4. Unique User Identification

7. Encryption and Decryption of Electronic Protected Health Information

12. Transmission Security to Guard Against Unauthorized Access to Information Transmitted Over an Electronic Communication Network

HHS POLICIES & PROCEDURES MANUAL

SUBJECT: Enforcement, Sanctions, and Penalties for Violations of Individual Privacy

POLICY NUMBER: 016-79-09-11

Table of Contents:

1. PURPOSE

The intent of this policy is to specify enforcement, sanction, penalty, and disciplinary actions that may result from violation of YCHHS policies regarding the privacy and protection of an individual's information and to offer guidelines on how to conform to the required standards.

2. General Procedures

A. **General:**

A.1. All employees, volunteers, interns, students, and members of the YCHHS workforce must guard against improper uses or disclosures of a YCHHS client or participant's information.

A.1.1. YCHHS employees, volunteers, interns, students, and members of the YCHHS workforce who are uncertain if a disclosure is permitted are advised to consult with a supervisor in the YCHHS workplace. The YCHHS Privacy Officer is a resource for any YCHHS workforce member that cannot resolve a disclosure violation question and may be consulted in accordance with the operational procedures of that YCHHS workplace.

B. **All employees are required to complete HIPAA training upon hire**, annually, and to be aware of their responsibilities under YCHHS privacy policies (See policy #016-79-04-32, *Mandatory Training and Tracking Requirements)*.

C. **Supervisors are responsible for assuring that employees who have access to confidential information**, whether electronic, hard copy, or orally, are informed of their responsibilities.

C.1. Staff will complete the online HIPAA training and test. Once completed the certification of completion will be electronically sent to the supervisor. These records shall be kept in the employees personnel file as well as tracked within YCHHS.

D. **YCHHS employees who violate** YCHHS policies and procedures regarding the safeguarding of an individual's information are subject to the Collective Bargaining Agreement and disciplinary action by YCHHS up to and including immediate dismissal from employment, and legal action by the individual.

E. **YCHHS workforce who knowingly and willfully violate** State or Federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.

F. **If YCHHS fails to enforce privacy safeguards**, YCHHS as a state agency may be subject to administrative penalties by the Department of Health and Human Services (DHHS), including federal funding penalties.

3. Retaliation Prohibited: Employees shall review policies on Electronic Communications with Clients and are required to comply with YCHHS policies related to Client signed consent for electronic communication as well as YCHHS and CMS requirements for documenting electronic communications with clients (See YCHHS policy #016-79-03-02, *Electronic Communications With or About Clients).*

A. **Neither YCHHS as an entity nor any YCHHS workforce member will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against(§164.316 and §164.530(g):**

A.1. Any individual for exercising any right established under YCHHS policy, or for participating in any process established under YCHHS policy, including the filing of a complaint with YCHHS or with DHHS.

A.2. Any individual or other person for:

A.2.1. Filing of a complaint with YCHHS or with DHHS as provided in YCHHS privacy policies;

A.2.2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to YCHHS policy and procedures; or

A.3. Opposing any unlawful act or practice, provided that:

A.3.1. The individual or other person (including a YCHHS workforce member) has a good faith belief that the act or practice being opposed is unlawful; and

A.3.2. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected information in violation of YCHHS policy.

4. Disclosures by Whistleblowers and Workforce Crime Victims

A. **A YCHHS workforce member or business associate/qualified service organization may disclose an individual's protected client information if (§164.502(j)(1):**

A.1. The YCHHS workforce member or business associate/qualified service organization believes, in good faith, that YCHHS has engaged in conduct that is unlawful or that otherwise violates professional standards or YCHHS policy, or that the care, services, or conditions provided by YCHHS could endanger YCHHS staff, persons in YCHHS care, or the public; and

A.2. The disclosure is to:

A.2.1. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of YCHHS;

A.2.2. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by YCHHS; or

A.2.3. An attorney retained by or on behalf of the YCHHS employee or business associate for the purpose of determining the legal options of the YCHHS employee or business associate with regard to this YCHHS policy.

B. **YCHHS workforce member may disclose limited protected information about an individual to a law enforcement official if the workforce member is the victim of a criminal act and the disclosure is (§164.502(j)(2); 42 CFR Part 2, §2.12(c)(5):**

B.1. About only the suspected perpetrator of the criminal act; and

B.2. Limited to the following information about the suspected perpetrator (§164.512(f)(2)(i):

B.2.1. Name and address;

B.2.2. Date and place of birth;

B.2.3. Social security number;

B.2.4. ABO blood type and rh factor;

B.2.5. Type of any injury;

B.2.6. Date and time of any treatment; and

B.2.7. Date and time of death, if applicable.

B.3. **Behavioral Health Only:** Please note that 42 CFR Part 2 states disclosure is limited to:

B.3.1. Circumstances of the incident;

B.3.2. Patient Status;

B.3.3. Name and Address;

B.3.4. Individual's last know whereabouts.

B.4. HIPAA and 42 CFR Part 2 also allow for disclosures to avert a serious threat to the premises of a Part 2 program or a workforce member (§164.512(j); §2.12(c)(5).

5. SANCTIONS FOR VIOLATING CLIENT PHI

A. **Violations:** YCHHS workforce who violate YCHHS policies and procedures regarding the safeguarding of an individual's information are subject to:

A.1. Appropriate disciplinary action by YCHHS, up to and including immediate dismissal from employment.

A.2. Legal action by the individual, who may want to pursue a tort claim against the State of Oregon or a lawsuit against the state and the workforce member.

B. **Knowingly Violate Policy:** YCHHS workforce who knowingly and willfully violate State or Federal law for improper invasions of personal privacy may be subject to:

B.1. Criminal investigation and prosecution, both by the State of Oregon and by the Federal government, depending on the nature of the violation. Federal and State law provides substantial fines and prison sentences upon conviction, depending on the nature and severity of the violation.

B.2. Civil monetary penalties that the federal Department of Health and Human Services (DHHS) may impose.

Reference(s): 45 CFR 164.530

Appendixes

- YCHHS Form: "Authorization for Release of Medical and/or Health Information"
- YCHHS Form # 1022: "Access to Records and Accounting of Disclosures Request"
- YCHHS Form: "Notice of Privacy Practices"
- YCHHS Form # 1011: "Restricting Use and Disclosures and Amending Protected Health Information Request"
- YCHHS Form #1021: "Disclosures Log/Release of Protected Health Information Tracking Log"
- YCHHS Form # 1012 "Consent to Treatment"

HEALTH AND HUMAN SERVICES DEPARTMENT

ADMINISTRATION – ADULT – COMMUNITY SUPPORT SERVICES – ENHANCED RESIDENTIAL OUTREACH – FAMILY & YOUTH – PUBLIC HEALTH – VETERANS & DISABILITY SERVICES

638 NE Davis Street • McMinnville, OR 97128
Phone (503) 434-7523 • Fax (503) 434-9846
TTY (800) 735-2900 • www.hhs.co.yamhill.or.us

Consent to Treatment Form

As a client of Yamhill County Health and Human Services you have the following rights and responsibilities related to your treatment.

A. I understand I have the right to:

1) Receive services that promote recovery, resiliency, wellness, independence; are person, youth and family-directed; and are culturally and trauma sensitive;
2) Choose from available services and supports, those that are consistent with the assessment and service plan, culturally competent, provided in the most integrated setting in the community and under conditions that are least restrictive to the individual's liberty, that are least intrusive to the individual and that provide for the greatest degree of independence;
3) Be treated with dignity and respect;
4) Participate in the development and periodic review of my service plan and reassessment of service and support needs, and receive a copy of the written service plan;
5) Have access to all covered services for which a person is eligible based on medical necessity and administrative rules;
6) Have all medically appropriate services explained by your health provider, including expected outcomes and possible risks;
7) Inspect Service Record in accordance with ORS 179.505;
8) Refuse participation in experimentation;
9) Receive medication specific to the individual's diagnosed clinical needs, including medications used to treat opioid dependence;
10) Receive prior notice of transfer, unless the circumstances necessitating transfer pose a threat to health and safety;
11) Be free from abuse or neglect and to report any incident of abuse or neglect without being subject to retaliation;
12) Have religious freedom;
13) Be free from seclusion and restraint;
14) Be informed at the start of services, and periodically thereafter, of the rights guaranteed;

15) Be informed of the policies and procedures, service agreements and fees applicable to the services provided, and to have a custodial parent, guardian, or representative, assist with understanding any information presented;
16) Be informed of suicide risk;
17) Have family and/or guardian involvement in service planning and service delivery;
18) Make a Declaration for Mental Health Treatment when legally an adult;
19) File a complaint or grievance against Yamhill County without fear of retaliation (for more detail, please see Notice of Privacy Practices);
20) Exercise all rights set forth in ORS 109.610 through 109.697 if a child, or ORS 426.385 if committed to Department of Human Services;
21) Exercise all rights described in this consent without any form of reprisal or punishment;
22) Request electronic methods of communication for information, such as emails or texts, as long as the method meets HIPAA privacy and security standards and the information does not constitute a Notice of Action regarding a denial of service;
23) Receive a Notice of Privacy Practices (the "Notice") that explains how my health information can be used with my consent and when Yamhill County may use or disclose my health information without my consent;
24) I understand that I can refuse to sign this consent and/or refuse treatment unless I am required by a court or legal guardian to accept services here;
25) If you are a YCCO member, you have the right to a second opinion by a participating provider within the network, or non-participating provider if a qualified participating provider is not available, at no cost to you as a member;
26) If you are a YCCO member, you may also refer to your Member's Handbook for additional rights;
27) If you are in the gambling program, and if it is clinically indicated, then there could be phone counseling.

B. I understand that by signing this consent my health information will be used for:

1) Treatment: In order to ensure coordination and delivery of services we may share information with other professionals within the Department to provide you with treatment services. The Health and Human Services Department includes the following programs: Abacus; Adult Behavioral Health (Chemical Dependency & Mental Health); Community Support Services; Veterans' and Disabilities' Services; Enhanced Residential & Outreach; Family and Youth; and Public Health. In the event one of these programs has more restrictive privacy rules, the more restrictive rule will be applied. If you participate in a program with more restrictive rules you will be given additional information describing your privacy rights.
2) For Payment: Yamhill County may use or disclose information to get payment or to pay for the health care services you receive. For example, we may provide health information to bill your health plan for health care provided to you.
3) For Health Care Operations: Yamhill County may use or disclose information in order to manage its programs and activities. For example, we may use your health information to review the quality of services you receive.

C. You the client have the responsibility to:

1) Actively seek to solve problems, to help develop goals and follow the service plan, to review and evaluate your progress toward your service plan, and to make changes with your therapist and prescriber when needed.
2) Schedule and keep your appointments. If you have to cancel an appointment, you are responsible to give at least 24 hours notice.
3) Take medications as prescribed by your prescriber(s) and notify them of any change in medications prescribed to you outside of Yamhill County Health and Human Services, if applicable.
4) Seek additional help for medical, mental health, alcohol or illegal drug problems as they may interfere with treatment already being provided.
5) Pay any fees at the time of service.
6) Make sure your children are not left in our waiting areas unsupervised.

If You Have a Complaint:

Definition: A complaint is when a client shares they are not satisfied with the services and/or supports of Yamhill County Health and Human Services (YCHHS);
Policy: YCHHS knows that disagreements can occur between clients and staff about services. Our goal is to encourage clients to voice their concerns and reach agreed upon solutions. A Committee reviews the complaints and solutions to find ways we can improve services. Clients have the right to share concerns without fear of punishment or retaliation.
Process: If you have a complaint, we invite you to talk with the staff person involved. If you want a solution to your complaint, please put the complaint in writing. You may request help from staff or a representative to share a complaint. For more information on filing a complaint please see the *Yamhill County Health and Human Services' Complaint Process*.

E. Privacy Rights: If you feel your Privacy Rights have been violated (see the *YCHHS Notice of Privacy Practices*) you may file a complaint with the Yamhill County Privacy Officer, The State of Oregon Department of Human Services, Governor's Advocacy Office or the U.S. Department of Health and Human Services, Office of Civil Rights. We can assist you in locating these offices.

F. Mandatory Abuse Reporting: YCHHS employees are mandated to report incidents of abuse or neglect that they have reasonable cause to believe occurred, as required by law. This may include release of protected health information.

G. Please let us know if you need any assistance in filing a complaint or have any questions

I _____ (client initials) understand that I have the right to refuse to sign this consent. If I refuse to sign this consent, or if I revoke this consent in the future, I understand that YCHHS will not provide any treatment to me or arrange for treatment on my behalf, except under certain emergencies or if otherwise required by law.

I _____ (client initials) have received a copy of the *Yamhill County HHS Complaint Process*.

I _____ (client initials) understand the above information about my rights and responsibilities.

I _____ (client initials) have been given a copy of the *Yamhill County HHS Notice of Privacy Practices*. I have had a chance to review these policies and ask any questions.

I _____ (client initials) was offered as a recipient of adult behavioral health services, written information about *Declaration for Mental Health Treatment*.

I _____ (client initials) understand that this consent will remain in effect until I provide notice that I would like this Consent to be discontinued or revoked.

I _____ (client initials) would like to opt in for telehealth/telemedicine treatment services, with the understanding as the method meets HIPAA privacy, 42 CFR Part 2, and security standards.

I hereby give my informed consent to treatment at Yamhill County Health& Human Services.

_____

PARENT/GUARDIAN/CLIENT SIGNATURE DATE

_____

WITNESS DATE

Health and Human Services Department

Access to Records and Accounting of Disclosures Request Form

Date of Request: _____

Individual's Name: _____
Last First Middle

Home Address: _____

_____

Home Phone: _____ **Date of Birth:** _____ **Client #:** _____

Client Records Request

If you would like this information, please consider the following:

- You may ask to access, look at or get information about yourself that is in YCHHS records.
- YCHHS may deny you access to your information if it was given to YCHHS by someone other than a health care provider, under the promise of confidentiality.

I ____ (client initials if appropriate) hereby request that YCHHS provide me with access to the following records **[please check all boxes that apply]**:

- ❑ My medical records.
- ❑ My billing records.
- ❑ Other personally identifiable information used by YCHHS to make decisions about me.

_____

Fees:

Fee for the cost of labor is $25.00 per hour plus an additional $.03 per page copied[1]

The fee for this request will be: _____

Accounting or List of Disclosures Request

If you would like this information, please consider the following:

- The list is free one time in any twelve-month period.
- YCHHS will not list disclosures made more than six years before your request.
- YCHHS will not list disclosures made earlier than **April 13, 2003**.
- YCHHS will only list disclosures of Protected Health Information not related to Treatment, Payment, or Health Care Operations.
- YCHHS will not list disclosures that you authorized.

Fees:

The first request in a 12-month period is Free; Subsequent requests within the same 12 month period are $6.00 **The fee for this request will be:_____**

I ____ (client initials if appropriate) would like to receive a list of disclosures of my Protected Health Information made by Yamhill County Health and Human Services (YCHHS).

Format: Please provide the requested Information to me in **[check the appropriate boxes]**

- ❑ paper form;
- ❑ pick-up or view the Requested Information at a mutually agreeable time and place;
- ❑ have the Requested Information mailed to me at the following address:

[1] This fee may be waived based on federal poverty guidelines

Time Period of Request:

I am interested in accessing or obtaining a copy of Requested Information relating to the time period from: _____ through _____.

By My Signature:

I understand that this request does not include information compiled in reasonable anticipation of (or for use in) a civil, criminal or administrative proceeding or as may otherwise be required by applicable law.

I understand that YCHHS may deny this request under limited circumstances under federal regulations governing the protection of personally identifiable health information. I further understand that, which I may have the right to have a denial of my request reviewed by a licensed health care practitioner selected by YCHHS who did not participate in Yamhill County's decision to deny my request.

I understand that YCHHS will notify me of its decision to approve or deny my request to access or obtain a copy of the Requested Information within thirty (30) days of receiving this request if the information is maintained or accessible on-site at YCHHS or within sixty (60) days if the Requested Information is not maintained or accessible on-site at YCHHS. If YCHHS is unable to comply with my approved request within the applicable time limit, it may extend the applicable deadline for up to thirty (30) days by notifying me in writing.

_____ _____

Signature of Patient (or Personal Representative) Date

_____ _____

Printed name of Personal Representative Relationship to Client

For Office Use Only:

Date of Action Taken: _____

☐ Approved _____

☐ Denied _____

☐ Delayed _____

☐ If delayed, we will act on your request by: _____

Comments: _____

_____ ***Staff Initials*** _____

Your Right to Access Your Information:

- You have a right to request access, look at or get information about yourself that is in DHS records.
- You have a right to have an answer to your request within 30 days. If the information is not at this location, you have the right to have an answer within 60 days. If there are delays in getting you the answer, you will be told. The delay cannot be more than 30 days. You will receive an answer in writing.
- You may be charged a fee, if you have accessed the same information within the past year.
- Your request may be denied if professionals involved in your case believe that access to your information could be harmful to you or others.
- The reviewer must decide, within a reasonable time, whether to approve or deny your request. You will get an answer in writing. The answer will include the reason for the decision.

Your Right to an Accounting of Disclosures:

- You have a right to request an accounting of disclosures made by DHS of your information.
- You have a right to have an answer to your request within 60 days. If there are delays in getting you the answer, you will be told. The delay cannot be more than 30 days. You will receive an answer in writing.
- Your first request for an accounting in a twelve-month period is free. You may be charged for additional requests in the same twelve-month period.

You have a right to file a privacy complaint:

Individuals can file privacy complaints with Yamhill County's Privacy Officer or with the U.S. Department of Health and Human Services, Office for Civil Rights.

Privacy complaints may be directed to any of the following:

Yamhill County

Yamhill County HHS **HIPAA Privacy Official** **627 NE Evans** **McMinnville, OR 97128**	**Yamhill County** **HIPAA Privacy Officer** **535 NE Fifth Street** **McMinnville, OR 97128**

U.S. Department of Health and Human Services, Office for Civil Rights

Medical Privacy, Complaint Division 200 Independence Avenue,
SW HHH Building, Room 509H
Washington, D.C. 20201 Phone: 866-627-7748
TTY: 886-788-4989 Email: www.hhs.gov/ocr

YAMHILL COUNTY

HEALTH AND HUMAN SERVICES DEPARTMENT

DISCLOSURES LOG
RELEASE OF PROTECTED HEALTH INFORMATION TRACKING LOG

Client Name: **Client DOB:**

Section 1: Accounting of Disclosures Log (information released without a signed authorization or consent. See age2)

Date Disclosed	Name & Location of Person/Entity Receiving PHI:	PHI/ Information Disclosed:	Purpose of Disclosure:	Disclosed By:

Section 2: IF Releasing Entire Medical Record please complete below (See page 2 for additional information)

Date	Reason Why

Section 3: Tracking Log of Information Released in Paper Format (See p 2 for additional information)

Date Disclosed	Staff Initials	Name & Location of Person/Entity Receiving PHI	PHI/ Information Disclosed:	Auth/ ROI Filed.	Verified Signature of Person Authorizing
				Yes / No	Yes / No
				Yes / No	Yes / No
				Yes / No	Yes / No
				Yes / No	Yes / No
				Yes / No	Yes / No
				Yes / No	Yes / No
				Yes / No	Yes / No
				Yes / No	Yes / No

I. Terms:

A. PHI = Protected Health Information

B. ROI = Release of Information

C. Auth = Authorization

II. Section 2 Instructions for Completing the Authorization Log:

A. What to Record?

1. record any disclosures of Protected Health Information not otherwise allowed:
   - **a.** by client's authorization
   - **b.** to carry out treatment, payment, or health care operations

B. Note the following:

1. Date of disclosure
2. Name & address, if known, of the individual or entity receiving the information
3. A brief description of the information (See examples below)
4. A brief explanation of the purpose (See examples below)
5. Signature of the person making the disclosure

C. Examples of PHI provided by YCHHS Staff needing to be accounted for:

1. Information to a public health official (other than staff employed for public health functions) such as the reporting of disease or injury.
2. Information in response to mandatory child or elder abuse reporting laws to an entity authorized by law to receive the abuse report.
3. Information about an individual that is ordered to be disclosed pursuant to a court order in a court case or other legal proceeding - include a copy of the court order with the accounting.
4. Information about an individual provided by YCHHS staff to avert a serious threat to health or safety of a person.
5. Information from an individual's records in relation to licensing or regulation or certification of a provider or licensee or entity involved in the care or services of the individual.

III. Section 3: Instructions for Completing the Tracking Log of Information Released in Paper Format:

A. What to Record?

1. Record any information you have released, from a client's file that you either faxed, emailed, or otherwise sent out in paper format. The purpose is tracking only the client information that has been physically released.

B. Note the following:

1. Date of disclosure
2. Name & address, if known, of the individual or entity receiving the information
3. A brief description of the information
4. Authorization/ROI Filed– Has the original or copy of the Authorization or Release of Information (ROI) been placed in the client's file?
5. Verified Signature of Person Authorizing - Has the signature of the person authorizing the release of the information been verified that they in fact are authorized to release such information?

HEALTH AND HUMAN SERVICES DEPARTMENT

ADMINISTRATION – ADULT – COMMUNITY SUPPORT SERVICES – ENHANCED RESIDENTIAL OUTREACH – FAMILY & YOUTH – PUBLIC HEALTH – VETERANS & DISABILITY SERVICES

627 NE Evans Street • McMinnville, OR 97128
Phone (503) 434-7523 • Fax (503) 434-9846
TTY (800) 735-2900 • www.hhs.co.yamhill.or.us

Your Information. Your Rights. Our Responsibilities.

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. **Please review it carefully.**

Your Rights

You have the right to:

- Get a copy of your paper or electronic medical record
- Correct your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a list of those with whom we've shared your information
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

➢ *See page 2 for more information on these rights and how to exercise them*

Your Choices

You have some choices in the way that we use and share information as we:

- Tell family and friends about your condition
- Provide disaster relief
- Include you in a hospital directory
- Provide mental health care
- Market our services and sell your information
- Raise funds

➢ *See page 3 for more information on these choices and how to exercise them*

Our Uses and Disclosures

We may use and share your information as we:

- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues
- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

➢ *See pages 3 and 4 for more information on these uses and disclosures*

Your Rights

When it comes to your health information, you have certain rights.
This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record	• You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you. Ask us how to do this. • We will provide a copy or a summary of your health information, usually within 30 days of your request. We may charge a reasonable, cost-based fee.
Ask us to correct your medical record	• You can ask us to correct health information about you that you think is incorrect or incomplete. Ask us how to do this. • We may say "no" to your request, but we will tell you why in writing within 60 days.
Request confidential communications	• You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address. • We will say "yes" to all reasonable requests.
Ask us to limit what we use or share	• You can ask us **not** to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care. • If you pay for a service or health care item out-of-pocket in full, you can ask us not to share that information for the purpose of payment or our operations with your health insurer. We will say "yes" unless a law requires us to share that information.
Get a list of those with whom we've shared information	• You can ask for a list (accounting) of the times we have shared your health information for six years prior to the date you ask, who we shared it with, and why. • We will include all the disclosures except for those about treatment, payment, and health care operations, and certain other disclosures (such as any you asked us to make). We will provide one accounting a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.
Get a copy of this privacy notice	• You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.
Choose someone to act for you	• If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information. • We will make sure the person has this authority and can act for you before we take any action.
File a complaint if you feel your rights are violated	• You can complain if you feel we have violated your rights by contacting us using the information on page 1. • You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Ave, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting **www.hhs.gov/ocr/privacy/hipaa/complaints/.** • We will not retaliate against you for filing a complaint.

Your Choices

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions.

In these cases, you have both the right and choice to tell us to:	• Share information with your family, close friends, or others involved in your care • Share information in a disaster relief situation *If you are not able to tell us your preference, for example if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.*
In these cases we *never* share your information unless you give us written permission:	• Marketing purposes • Sale of your information • Most sharing of psychotherapy notes

Our Uses and Disclosures

How do we typically use or share your health information?

We typically use or share your health information in the following ways.

Treat you	• We can use your health information and share it with other professionals who are treating you.	***Example:*** *A doctor treating you for an injury asks another doctor about your overall health condition.*
Run our organization	• We can use and share your health information to run our practice, improve your care, and contact you when necessary.	***Example:*** *We use health information about you to manage your treatment and services.*
Bill for your services	• We can use and share your health information to bill and get payment from health plans or other entities.	***Example:*** *We give information about you to your health insurance plan so it will pay for your services.*

continued on next page

How else can we use or share your health information? We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health and research. We have to meet many conditions in the law before we can share your information for these purposes. For more information see: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.**

Help with public health and safety issues	• We can share health information about you for certain situations such as: • Preventing disease • Helping with product recalls • Reporting adverse reactions to medications • Reporting suspected abuse, neglect, or domestic violence • Preventing or reducing a serious threat to anyone's health or safety
Do research	• We can use or share your information for health research.
Comply with the law	• We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we are complying with federal privacy law.
Respond to organ and tissue donation requests	• We can share health information about you with organ procurement organizations.
Work with a medical examiner or funeral director	• We can share health information with a coroner, medical examiner, or funeral director when an individual dies.
Address workers' compensation, law enforcement, and other government requests	• We can use or share health information about you: • For workers' compensation claims • For law enforcement purposes or with a law enforcement official • With health oversight agencies for activities authorized by law • For special government functions such as military, national security, and presidential protective services
Respond to lawsuits and legal actions	• We can share health information about you in response to a court or administrative order, or in response to a subpoena.

I. Yamhill County Health & Human Services (YCHHS) may only use or release substance abuse records if the person or business receiving the records has a specialized agreement with YCHHS.

II. YCHHS follows the requirements of federal and state privacy laws including laws about protecting information related to drug and alcohol abuse and treatment and mental health condition and treatment.

III. If YCHHS releases information to someone else with your approval, the information may not be protected by the privacy rules and the person receiving the information may not have to protect the information. They may release your information to someone without your approval.

Our Responsibilities

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: **www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.**

Changes to the Terms of this Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Approved by: Silas Halloran-Steiner, Yamhill County HHS Director
May 15, 2015

This Notice of Privacy Practices applies to the following organizations.

This notice applies to Yamhill County Health & Human Services and its business associates.

To use any of the privacy rights listed above or to request this notice in Spanish or other format, you may contact:
Telephone: 503-434-7523
Fax: 503-434-9846
TTY: 1-800-735-2900

Authorization for Use and Disclosure of Information

This form is available in alternative formats including large print, Spanish and oral presentation.

Legal last name of client/applicant:	**First:**	**MI:**	**Date of Birth:**
Other names used by client/applicant:			**Case ID number:**

By signing this form, I authorize the following record holder to disclose the following specific confidential information about me:

Release from one record holder: *(individual, school, employer, agency, medical or other provider)*	**Release To:** *(Address required if mailed. If releasing to a team, list members)*

I authorize a mutual exchange of the information listed below between parties**:** **YES** **NO**

If the information contains any of the types of records or information listed below, additional laws relating to use and disclosure may apply. I understand that this information will not be disclosed unless I place my initials in the space next to the information:

Mental Health		Alcohol /Drug		Gambling		HIV/ AIDS		Genetic Testing	

Specific Information to be Disclosed:

Records Dated From: To:

Purpose:	

This authorization is valid for one year from the date of signing unless otherwise specified below.

Expiration date or event: 90 days after client closes to services

Signature & Copies:

I was given the opportunity to ask questions about this form and what it does. I can cancel this authorization at any time. The cancellation will not affect any information that was already disclosed. I understand that state and federal law protects information about my case. I understand what this agreement means and I approve of the disclosures listed. I am signing this authorization of my own free will. I understand that the information used and disclosed as stated in this authorization may be subject to re-disclosure and no longer protected under federal or state law. I also understand that federal or state law prohibits re-disclosure of HIV/AIDS, mental health and drug/alcohol diagnosis, treatment, vocational rehabilitation records or referral information without specific authorization.

Full legal signature of individual or authorized personal representative:	**Relationship to client:**	**Date:**

	☐ Legal Rep. Documentation on File	
Name of staff person (print):	**Initiating agency**	**Date:**
This is a true copy of the <u>original</u> authorization document.		

Required information for the client

To provide or pay for health services: If the Yamhill County Health and Human Services (YCHHS) is acting as a **provider** of your health care services or paying for those services under the Oregon Health Plan or Medicaid Program, you may choose not to sign this form. That choice **will not** adversely affect your ability to receive health services, *unless* the health care services are solely for the purpose of providing health information to someone else and the authorization is necessary to make that disclosure. *(Examples of this would be assessments, tests or evaluations.)* Your choice not to sign **may affect** payment for your services if this authorization is necessary for reimbursement by private insurers or other non-governmental agencies.

This is a voluntary form. YCHHS cannot condition the provision of treatment, payment or enrollment in publicly funded health care programs on signing this authorization, except as described above. However, you should be given accurate information on how refusal to authorize the release of information may adversely affect eligibility determination or coordination of services. If you decide not to sign, you may be referred to a single service that may be able to help you and your family without an exchange of information.

Using this form

1. **Terms used: Mutual exchange:** A "yes" allows information to go back and forth between the record holder and the people or programs listed on the authorization. **Team:** A number of individuals or agencies working together regularly. The members of the team must be identified on this form.
2. **Assistance:** Whenever possible, a YCHHS staff person should fill out this form with you. **Be sure you understand the form before signing.** Feel free to ask questions about the form and what it allows. You may substitute a signature with making a mark or by asking an **authorized** person to sign on your behalf.
3. **Guardianship/custody:** If the person signing this form is a personal representative, such as a guardian, a copy of the legal documents that verify the representative's authority to sign the authorization must be attached to this form. Similarly, if an agency has custody and their representative signs, their custody authority must be attached to this form.
4. **Cancel:** If you later want to cancel this authorization, contact your YCHHS staff person. You can remove a team member from the form. You will be asked to put the cancellation request in writing.
   Exception: Federal regulations do not require that the cancellation be in writing for the Drug and Alcohol Programs. No more information can be disclosed or requested after authorization is cancelled. YCHHS can continue to use information obtained prior to cancellation.
5. **Minors:** If you are a minor, you may authorize the disclosure of mental health or substance abuse information if you are age 14 or older; for the disclosure of any information about sexually transmitted diseases or birth control regardless of your age; for the disclosure of general medical information if you are age 15 or older.
6. **Special attention:** For information about **HIV/AIDS, mental health, genetic testing or alcohol/drug abuse or gambling**, the authorization must clearly identify the specific information that may be disclosed and the purpose.

Redisclosure:

This record which has been disclosed to you is protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of this record unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or, is otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see §2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§2.12(c)(5) and 2.65.