BEFORE THE BOARD OF COUNTY COMMISSIONERS

FOR COLUMBIA COUNTY, OREGON

In the Matter of Adopting Columbia County HIPAA Policy Updated for the HIPAA Omnibus Final Rule and Directing the Appointment of the County Privacy Officer and County Security Officer	ORDER NO. 69-2020

WHEREAS, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations establish standards to protect the privacy of medical records and other individually identifiable health information; and

WHEREAS, Columbia County is a "hybrid entity" under 45 CFR §§ 164.103 and 164.105 of HIPAA because some County departments use and disclose individually identifiable health information, including protected health information, while other County departments do not; and

WHEREAS, as a hybrid entity, the County must adopt and implement policies on the use and disclosure of protected health information; and

WHEREAS, on April 9, 2003, the Board of County Commissioners approved Order No. 25-2003, "In the Matter of Adopting Policy on Compliance with HIPAA, Designating County Health Care Components, Designating a Privacy Officer and Contact Persons"; and

WHEREAS, the HIPAA Omnibus Final Rule, adopted in 2013, implements provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which strengthens privacy and security protections for health information; and

WHEREAS, the County's HIPAA policy must be updated to incorporate the requirements of the Final Rule; and

NOW, THEREFORE, THE COLUMBIA COUNTY BOARD OF COMMISSIONERS HEREBY ORDERS, as follows:

1. The Columbia County Health Insurance Portability and Accountability Act (HIPAA) Policy, attached hereto as Exhibit A and incorporated herein by this reference, is hereby adopted.

2. Columbia County is designated as hybrid entity under HIPAA, and Attachment A to Exhibit A identifies the County Departments that are "Covered Components" and "Business Associates" for purposes of HIPAA:

3. Each Department that is a Covered Component shall designated a privacy manager for that component who shall be designated as that department's contact for matters relating to HIPAA, including complaints of any breach or potential breach of information under HIPAA.

4. Robin McIntyre, Senior Assistant County Counsel, shall serve as the County's Privacy Officer for HIPAA purposes.

5. Holly Miller, Information Technology Director, shall serve as the County's Security Officer for HIPAA purposes.

6. Order No. 25-2003 is hereby repealed.

DATED this 15 day of July, 2020.

BOARD OF COUNTY COMMISSIONERS
FOR COLUMBIA COUNTY, OREGON

By: _____
Alex Tardif, Chair

By: _____
Margaret Magruder, Commissioner

By: _____
Henry Heimuller, Commissioner

Approved as to form

By: _____
Office of County Counsel

EXHIBIT A

COLUMBIA COUNTY
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) POLICY

Purpose: This Policy outlines the general guidelines and expectations governing requests for, access to, and use and disclosure of Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).

1. OVERVIEW / APPLICABILITY

Overview: HIPAA was enacted to increase the portability of health insurance, increase the accountability of the health insurance industry, and provide administrative simplification to the healthcare industry. Administrative simplification includes making it easier and more efficient to share "protected health information" (PHI) electronically. In conjunction with that, however, significant and far-reaching privacy and security standards are imposed on many entities that use or maintain such information. HITECH was enacted to address the privacy and security concerns associated with the electronic transmission of health information. HITECH also extends the complete Privacy and Security Provisions of HIPAA to Business Associates of covered entities.

Applicability: Columbia County has designated itself as a "hybrid covered entity." This means certain portions of the County are "Covered Components" and directly subject to HIPAA. Other parts are not subject to HIPAA, generally, because they are not a healthcare provider, do not perform covered transactions as defined under HIPAA, and do not have access to, use or disclose PHI.

Unless otherwise specified, this Policy applies only to those departments or programs designated as HIPAA "Covered Components" as set forth in Attachment A. The County Privacy Officer shall maintain a list of departments or programs considered to be Covered Components under the hybrid covered entity, and amend the list of Covered Components as realignments occur and program offerings change within the County. Covered Components are prohibited from disclosing PHI to non-Covered Components, except as permitted by this Policy or required/permitted by applicable law.

Certain non-Covered Components may have HIPAA obligations as "Business Associates," described further in *Section 23*.

HIPAA does not apply to employee medical information held and used by the County as an employer.

Relationship to other laws and policies:
45 CFR 160.201 through 205
This Policy must be considered in addition to all other statutes, administrative rules, or other provisions relating to privacy or confidentiality of personal information. In general, the provision that imposes the greatest degree of confidentiality to the individual prevails, except as

noted below. In particular, note that ORS 179.505 and 42 CFR Part 2 impose restrictions on disclosure that are in some cases stricter than HIPAA.

Nothing in this Policy shall be construed as conflicting with the terms of HIPAA, HIPAA Privacy Regulations 45 CFR Parts 160 and 164, HITECH or the HIPAA Breach Notification Rule. Those regulations shall be consulted as necessary in conjunction with this Policy.

Implementing Procedures:
All Covered Components should consider adopting additional procedures to implement this Policy. All such procedures, when modified, shall continue to be reviewed by the County Privacy Officer and, when appropriate, the Office of County Counsel.

County Privacy Officer:
45 CFR 164.530(a)(1)
The County shall name a countywide Privacy Officer. Each Covered Component shall designate a Privacy Manager. The Privacy Manager shall be responsible for implementing and ensuring compliance with this Policy and more specific procedures applicable to individual Covered Components. Workforce Members of the Covered Component shall address issues regarding privacy of PHI to their Privacy Manager who, when appropriate, shall in turn refer the matter to the County Privacy Officer or Office of County Counsel.

The County Privacy Officer must immediately be notified upon any inquiry by or from the Secretary of the U.S. Department of Health and Human Services or its designee.

Training:
45 CFR 164.530(a)(2)
Each Covered Component must train all of its Workforce Members in HIPAA, this Policy, and the procedures of each Covered Component within thirty (30) calendar days of hire. The County Privacy Officer must approve training. The detail level may vary depending on the duties and responsibilities of the Workforce Member, but must be adequate to help protect against unauthorized uses and disclosures of PHI. Workforce Members who are promoted or have duties reassigned must be trained on any newly relevant policies and procedures within thirty (30) calendar days of reassignment.

Completion of training must be documented and retained. Tracking of training completion shall be maintained by the County Privacy Officer. Privacy Managers that deliver training at the Covered Component level shall share training logs with the County Privacy Officer.

The Privacy Officer shall require Workforce Members to complete annual refresher training. The training may be available online. Additionally, all Workforce Members shall review this Policy and Covered Component procedures once a year.

Privacy Managers are responsible for monitoring and ensuring that Workforce Members in their Covered Components have completed training within the required timeframes. Privacy Managers will escalate to department leadership as necessary to ensure that training is completed.

2. DEFINITIONS

The following are terms commonly referenced in this Policy. In the event of conflict or absence of a term, the definitions set forth in HIPAA and the implementing federal privacy rules, 45 CFR 160, 164, shall govern:

Breach: The impermissible acquisition, access, use or disclosure of unsecured PHI in any form or medium, including electronic, paper or oral form which compromises the security or privacy of such information.

Business Associate: A third party that creates, receives, maintains or transmits PHI on behalf of a covered entity or provides a service to a covered entity. Business Associates are commonly third parties that, on behalf of the Covered Component, assist, arrange, or perform a support service that involves the use or disclosure of PHI, including claims processing or administration, data analysis, utilization review, quality assurance, billing assurance, billing, benefit management, practice management, repricing and legal, accounting, and accreditation services. A healthcare provider that the Covered Component retains by contract to provide treatment to an Individual and for which the Covered Component pays is NOT a Business Associate. *See Sec. 23*

Complaint: An expression of dissatisfaction or concern with the County's compliance with HIPAA in terms of the use or disclosure of PHI. A Complaint may be informal (verbal) or formal (in writing). After investigation, the basis for a Complaint may be determined to also be a Breach.

Covered Component: A department or other unit of the County that is subject directly to HIPAA and this Policy and has the same meaning as the term "health care component" as defined in CFR 164.103. *See* Attachment A for a list of the County's "Covered Components."

Designated Record Set:

Each Covered Component will retain the Designated Record Set for the Covered Component. The Designated Record Set includes the following:

- The medical records and billing records about Individuals maintained by or for a covered healthcare provider
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan
- Records used, in whole or in part, by or for the Covered Component to make decisions about Individuals

A "record" is any item, collection, or grouping or information that includes PHI and is maintained, collected, used or disseminated by or for a covered entity. A "decision" includes non-healthcare decisions about the Individual.

Designated Record Set is defined in 45 CFR 164.501.

Disclose: Release, transfer, relay, provision of access to, or conveying of PHI to any Individual or entity outside of the County.

Healthcare: Care, services, or supplies related to the health of an Individual. Includes but is not limited to: Preventative, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, counseling, service, assessment or procedure relating to the physical or mental condition, or functional status, or that affects the structure or function of the body.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, as amended. Public Law 104-191.

HITECH: The Health Information Technology of Clinical Health Act. Public Law 111-5 § 2.A.III and B.4.

Impermissible: Acquisition, access, use or disclosure of PHI that is not permitted under HIPAA.

Incident: An issue, event, question or concern related to PHI that is not determined to be a Complaint or a Breach.

Incidental Disclosure: A secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure.

Individual: The person whose PHI is at issue.

Protected Health Information (PHI): Individually identifiable health information, including demographic information, created or received by the Covered Entity that relates to the past, present, or future physical or mental health or condition of an Individual; the provision of healthcare to an Individual; or the past, present, or future payment for the provision of healthcare to an Individual. Further, PHI includes information that either identifies the Individual, or there is a reasonable basis to believe the information can be used to identify the Individual. PHI does not include information of an Individual that has been deceased for 50 years or more. PHI includes electronic PHI (ePHI).

Secretary: The Secretary of the U.S. Department of Health and Human Services or designee.

Unsecured Protected Health Information (PHI): PHI that is not encrypted or destroyed.

Use: The sharing, utilization or analysis of PHI within a Covered Component.

Workforce Member: An employee, volunteer, student, intern or other person employed by or performing services for a Covered Component of the County.

3. REQUESTS FOR, AND USE OF, PHI BY WORKFORCE MEMBERS

A. PHI shall not be accessed, requested or used by Workforce Members in a manner, or for a purpose, which would be inconsistent with the policies governing use or disclosure of PHI set forth below.

B. Requests for PHI by Workforce Members shall be limited to the minimum necessary to perform the work for which the PHI is requested. Specific records, rather than the entire file,

shall be requested in accordance with the minimum necessary standard. De-identified information shall be requested when practicable.

4. USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

PHI held by a Covered Component shall not be used or disclosed except for the following permissible uses and disclosures. Note that there may be further restrictions to the permissible uses and disclosures described below by other state or federal laws, the Notice of Privacy Practices (Section 9), or an authorization by the Individual (Section 10). Special provisions govern inmates (Section 15), decedents (Section 16), psychotherapy notes (Section 17), and deidentified PHI (Section 21).

A. To the Individual:
45 CFR 164.502(a), 45 CFR 164.524

Except for the following, an Individual has a right to access, inspect and copy his or her own PHI, notwithstanding anything to the contrary in state law:

1. Psychotherapy notes. *See Sec. 17*

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

3. Persons in custody (inmates). *See Sec. 15*

4. Possible danger to others or self. *See Sec. 4.*

See Sec. 12, for permissible conditions on access to an Individual's own PHI.

B. To the personal representative of the Individual (adult or minor).
See Sec. 6.
45 CFR 164.502(g)

C. To persons involved in the Individual's care or payment for care, such as family and close friends, as follows:
45 CFR 164.510(b)

1. When the Individual is present and able to make healthcare decisions and one of the following occurs:

   a. the Individual consents,

   b. the Individual is given opportunity to object and does not, or

   c. the Individual does not object and permission can reasonably be inferred from the circumstances.

2. When the Individual is not present, incapacitated, or there is an emergency, disclosure is permitted if, in the Workforce Member's professional judgment in light of common practice, disclosure is in the best interest of the Individual and is limited to information directly relevant to the person's involvement. This includes the Individual's location, general condition, or death, such as in an emergency and includes permitting the person to pick up PHI on behalf of the Individual.

3. To a public or private entity authorized by law or charter to assist in disaster relief (*e.g.,* Red Cross) for coordinating permissible disclosures to persons involved in the Individual's care. The rules set forth above for disclosures to persons involved in the Individual's care apply.

4. Limitations on Use and Disclosure: Where applicable, and after obtaining an Authorization to do so, Workforce Members may disclose only that portion of the PHI that is specified by the Individual or, in the absence of a specification, is relevant to the Individual's condition and care.

    a. Workforce Members shall not assume that an Individual's Authorization or lack of objection implies agreement to disclose PHI indefinitely in the future.

    b. Workforce Members shall not disclose the Individual's HIV/AIDS, genetic, alcohol or drug treatment, sexual assault or child abuse history, unless an Authorization is obtained specifying disclosure of this information, or unless otherwise permitted by Oregon or federal law regulating these categories.

D. To persons described in a properly executed voluntary authorization. Generally, Individuals may authorize use or disclosure of the Individual's own PHI for any purpose specified in the authorization. Note: An authorization is not the same as a consent to treatment form. 45 CFR 164.502(a), 45 CFR 164.508

E. For treatment to others within the Covered Components of the County and to another healthcare provider. Treatment includes the provision, coordination or management of healthcare and related services by one or more cooperating healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to an Individual; or the referral of an Individual for healthcare from one healthcare provider to another. Use (not disclosure) is subject to minimum necessary standards. *See Sec. 7,* 45 CFR 164.502(a), 45 CFR 164.506(c)

F. For payment to others within the Covered Components of the County, to another covered entity or healthcare provider. Payment refers to the activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; including activities associated with reimbursement for the provision of healthcare. Includes:

1. Activities related to the determination of eligibility or coverage and adjudication of health benefit claims;

2. Review of healthcare services with respect to medical necessity;

3. Coverage under a health plan, and appropriateness of care;

4. Utilization review activities, including pre-authorization of services, concurrent and retrospective review of services; and

5. Disclosure to consumer reporting agencies relating to reimbursement.

Minimum necessary standards apply. *See Sec. 7.* 45CFR 164.502(a), 45 CFR 164.506(c)

G. For healthcare operations within the Covered Components of the County or with other Covered Entities. Healthcare operations includes a wide range of activities that make up the typical functions of a healthcare or service operation, including quality assessment and improvement, protocol development, case management, peer review, performance evaluation, training programs, legal and auditing services. Also included is due diligence for merger, transfer or consolidation of an agency as well as certain uses for fundraising. A Covered Component may use and disclose PHI with another third party covered entity (or County covered component) only if both the Covered Component and the covered entity/Covered Component had or have a relationship with the common Individual, the PHI pertains to that relationship, and the disclosure is for:

1. specified activities including quality assessment, certain population based activities such as cost containment, protocol development, case management or care coordination, contacting providers or Individuals about treatment alternatives, professional competence evaluations, training, or credentialing; or

2. fraud and abuse detection and compliance.

Minimum Necessary standards apply. *See* Sec. 7.45 CFR 164.502(a), 45 CFR 164.506(c)

H. To a Business Associate of the Covered Component if the Business Associate satisfactorily assures that it will appropriately safeguard the information. *See Sec. 13* Minimum Necessary standards apply. *See Sec. 7,* 45 CFR 164.504(e)

I. To report child abuse as required by law. Disclosure of PHI for child abuse reporting is not subject to the rules governing adult abuse reporting in paragraph J below. Document these disclosures. *See Sec.* 5, 45 CFR 164. 512(b)(1)(ii)

J. To report abuse, neglect, or domestic violence involving adults to a government authority authorized by law to receive such reports. 45 CFR 164.512(c)

1. If reporting is mandated by law, follow the relevant law. Do not disclose more than required by the law.

2. If reporting is not mandated by law, Minimum Necessary standards apply and PHI may be disclosed only if the victim consents or:

   a. in the exercise of professional judgment, disclosure is necessary to prevent serious harm, or

b. PHI is requested by law enforcement and the official represents that the PHI is not intended to be used against the Individual and that failure to disclose the PHI promptly would materially adversely affect a law enforcement action.

Document the request and disclosure.

3. The Individual or personal representative shall be informed of all such disclosures unless:

   a. a Workforce Member, in the exercise of professional judgment, thinks that informing the Individual would place the Individual, or another person, at risk of serious harm, or

   b. a Workforce Member thinks that the personal representative is responsible for the abuse or neglect and informing the personal representative would not be in the best interests of the Individual.

   Document the request and disclosure. *See Sec. 5.*

K. To a public health authority for public health purposes such as preventing or controlling disease, injury, or disability or conducting public health surveillance, investigations, and interventions; reporting vital events such as births and deaths; child abuse reports. Minimum Necessary standards apply to any such disclosure not required by law. *See Sec. 7.*

Document the request and disclosure. *See Sec. 5.* 45 CFR 164.512(b)(1)(i)

L. To a person who may have been exposed to a communicable disease or otherwise may be at risk of contracting or spreading a disease or condition, if the disclosure is authorized by law. Minimum Necessary standards apply. *See Sec. 7*

Document the request and disclosure. *See Sec. 5.* 45 CFR 164.512(b)(1)(iv)

M. Disclosures to other Covered Components and support services within the County to carry out healthcare operations. Examples include to Information Technology Services for computer/program troubleshooting; to County Counsel for legal advice; to Archives for records retention purposes. Minimum Necessary standards apply. *See Sec. 7.*

N. For judicial and administrative proceedings.
45 CFR 164.512(e)

County counsel must always be consulted before making any disclosure listed in this subsection below.

1. As expressly ordered by a court or administrative tribunal.

2. A civil subpoena, request for production of documents, or similar discovery process not signed by a judge, provided that the person seeking the information represents in writing and provides supporting documentation, that:

a. The person has made a good faith attempt to provide the Individual with written notice about the request and an opportunity to object, the time for objecting has expired and no objections were filed, or any objections were resolved and the request is consistent with that resolution; or

b. The person has obtained or is in the process of obtaining a qualified protective order that limits use of the PHI to the dispute at issue and requires return or destruction of the PHI when done.

Document the request and disclosure. *See Sec. 5.*

O. To law enforcement if:
45 FR 164.512(f)

1. Required by law. Only disclose what is required. Document the request and disclosure.

2. In compliance with the express terms of a court ordered warrant, HIPAA-compliant subpoena, or summons; a grand jury subpoena; or other process authorized by law, provided that:

   a. the PHI is relevant and material to a legitimate law enforcement inquiry;

   b. the request is specific and limited in scope to the extent reasonably practicable for the purpose for which it is sought; and

   c. de-identified information could not reasonably be used.

Note: County Counsel must review all subpoenas for PHI. Document the request and disclosure.

3. In response to a request for assistance in identifying or locating a suspect, fugitive, material witness, or missing person, the following may be disclosed:

   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 or death
   g. distinguishing physical characteristics

This exception does not permit disclosure of DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or typing.

Note: The County is not in violation of HIPAA if a Workforce Member who is a victim of a crime discloses any of the above-listed PHI relating to the suspected perpetrator to law enforcement. 45 CFR 164.502(j)(2)

4. In response to a request for PHI about an Individual who is or is suspected to be a victim of a crime if:

   a. the Individual consents, or

   b. the Individual's consent cannot be obtained due to incapacity or other emergency circumstances and the law enforcement official represents that:

      i. The PHI is necessary to determine whether a violation by a person other than the victim occurred and the PHI is not intended to be used against the victim;

      ii. Immediate law enforcement activity that depends on the PHI would be materially and adversely affected by waiting; AND

      iii. The disclosure is in the best interest of the victim, in the professional judgment of the Covered Component.

   c. The Covered Component must inform the Individual that a report has been (or will be) made unless:

      i. in its professional judgment, the Covered Component believes that informing the Individual would place the Individual at risk of serious harm; or

      ii. the Covered Component would be informing a personal representative whom the Covered Component believes to be responsible for the abuse, neglect, or other injury and the Covered Component reasonably believes in its professional judgment that informing such personal representative would not be in the Individual's best interest.

   Document the request and disclosure.

5. Disclosure of PHI about a decedent is necessary to alert law enforcement, if there is a suspicion that death may have resulted from criminal conduct.

6. A good faith reason exists to believe that PHI constitutes evidence of a crime occurring on County property.

7. An emergency healthcare provider may disclose PHI to law enforcement, if necessary to alert them to a crime, its location, or the perpetrator.

   Minimum Necessary standards apply unless law requires the disclosure. *See Sec. 7.*

   Document request and disclosure. *See Sec. 5.*

P. To health oversight agencies for oversight purposes authorized by law, or other activities necessary for appropriate oversight of the following:

1. Healthcare system;

2. Government benefit programs for which health information is relevant to beneficiary eligibility;

3. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or

4. Entities subject to civil rights laws under which health information is necessary for determining compliance.

Disclosure is not permitted if:

1. the Individual is the subject of the investigation, and

2. the investigation arises out of or is directly related to some purpose other than to a claim for, the receipt of, or the Individual's qualifications for healthcare or public benefits and services.

Document request and disclosure. *See Sec. 5.* 45 CFR 164.512(j)

Q. Avert a serious and imminent threat to health or safety.
45 FR 164.512(j)

1. If consistent with applicable law and ethical standards and there is a good faith belief that the use or disclosure is:

   a. necessary to prevent or lessen a serious and imminent threat to health or safety of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat (including the target of the threat), or

   b. necessary for law enforcement to identify or apprehend an Individual where the Individual has admitted participation in a violent crime reasonably believed to have caused serious physical injury. Only disclose the statement and the PHI listed in O.3 above. Use or disclosure is not permitted, if the information was obtained by the Covered Component:

      i. during treatment for the propensity to commit the criminal conduct at issue, counseling, or therapy, *or*

      ii. through a request by the Individual for referral to treatment for the propensity, counseling, or therapy.

   c. necessary for law enforcement to identify or apprehend an Individual who has escaped from lawful custody. Minimum Necessary standards apply. *See Sec. 7.*

Document the request and disclosure. *See Sec. 5*

R. Government Public Benefits Programs
45 CFR 164.512(k)(6)

A government entity that is a health plan providing public benefits may disclose PHI regarding eligibility and enrollment with another government agency administering a government public benefit program, if the sharing (including a shared database) is authorized by statute or administrative rule. Minimum Necessary standards apply. *See Sec. 7.*

A covered government entity that administers a public benefit program may disclose PHI to another covered government entity that provides public benefits to a same or similar population to the extent necessary to coordinate and improve the administration and management of the public benefit programs.

S. Miscellaneous Governmental Purposes.
45 FR 164.512(k)

1. As required by the U.S. Department of Health and Human Services, minimum necessary standard does not apply.

2. Disclosure of PHI of armed forces personnel deemed necessary by the appropriate military command.

3. National and presidential security and intelligence activities authorized by the National Security Act (50 USC 401, et. seq.).

4. Whistleblowers may be protected against a claim of violation of HIPAA, if they qualify under 45 CFR 164.502(j)(1).

5. To the Food and Drug Administration (FDA), if the Individual is subject to FDA jurisdiction pursuant to 45 CFR 164.512(b)(iii).

6. For research pursuant to 45 CFR 164.512(i).

7. Authorized and to the extent necessary to comply with workers' compensation laws. (**Note:** HIPAA does not apply to employment records of County employees.) A Covered Component may disclose PHI other than drug and alcohol treatment records as authorized by, and to the extent necessary to comply with laws relating to workers' compensation or other similar programs. However, HIV related information is only released when a claim for workers' compensation benefits is made for HIV or AIDS or when such information is directly relevant to the claimed conditions, (OAR 436-010-0240(1)).

Document all of these requests and disclosures, except 3. *See Sec. 5*

T. To report information to the Individual's employer if:

1. The Covered Component provides a healthcare service to the Individual at the request of the employer either to conduct an evaluation relating to medical surveillance of the workplace or evaluate whether the Individual has a work-related illness or injury.

2. The PHI that is disclosed consists of findings of a workplace medical surveillance concerning work-related illness or injury.

3. The employer needs such findings in order to comply with its obligations under OSHA or the Mine Safety and Health Act, or under any state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance.

Covered Components will provide written notice to the Individual of what PHI relating to the workplace medical surveillance is disclosed to the employer by giving a copy of the notice to the Individual at the time the healthcare is provided or if the healthcare is provided on the worksite of the employer, by posting the notice in a prominent place at the location where the healthcare is provided.

U. Immunizations: A Covered Component may disclose proof of immunization to a school where state or other law requires the school to have such information prior to admitting the student. The Covered Component must obtain agreement, which may be oral, from a parent, guardian or other personal representative of the Individual or from the Individual himself or herself if the Individual is an adult or emancipated minor. Verbal agreement must be documented.

5. DOCUMENTING AND ACCOUNTING FOR DISCLOSURES

45 CFR 164.528

A. HIPAA requires that certain disclosures be documented and that an Individual has a right to an accounting of those disclosures. These are:

1. To a public health authority or other appropriate government authority authorized by law to report child or other abuse, neglect, or domestic violence. **Note:** State law allows for keeping confidential the name of the person who reported child abuse.

2. To a public health authority that is authorized by law to collect information for the purpose of preventing or controlling disease, injury or disability.

3. To health oversight agencies (*e.g.*, audits, licensing and disciplinary actions, investigations).

4. For judicial and administrative proceedings, including all court orders and subpoenas.

5. To law enforcement regarding:

   a. crime on the premises;
   b. emergencies when crime is suspected;

c. wound or injury reports; or
d. identifying or locating a suspect or fugitive.

6. Reports about decedents to medical examiners, or funeral homes.

7. Workers' Compensation (except regarding County employees).

8. To correctional institutions—unless the Individual is in custody.

9. To appropriate United States or foreign military command authorities regarding an Individual who is a member of United States or foreign armed forces.

10. To a person subject to the jurisdiction of the Food and Drug Administration.

11. Pursuant to a waiver of the authorization requirement for the use and disclosure of PHI for research purposes.

12. To a person who may have been exposed to a communicable disease.

13. Any unlawful, unauthorized, or impermissible disclosure (privacy or security breach or incident) or under a defective Authorization.

14. Disclosure or use of psychotherapy notes.

15. To authorized federal government officials for the provision of protected services to the President of the United States and others.

16. To an employer about an Individual who is a Workforce Member, in connection with medical surveillance of the workplace or to evaluate a work-related illness or injury.

17. To a third party (emergency personnel) to prevent an imminent and serious threat to health or safety.

Disclosures to or by a Business Associate that fall within this list must be documented. The County, not the Business Associate, is legally responsible for providing the accounting of disclosures.

B. Examples of common permitted disclosures that do not need to be documented or accounted for (including to or by a Business Associate) are:

1. For treatment, payment or healthcare operations.

2. To the Individual or authorized by the Individual.

3. Incidental Disclosures both within and outside the Covered Component.

4. To persons involved in the Individual's care or payment for care (*e.g.,* family or close personal friends).

5. National security or intelligence purposes.

6. To correctional institutions, if the Individual is in custody.

7. Disclosures made prior to six (6) years before the date of the request.

8. Disclosures as part of a limited data set.

9. Disclosures pursuant to a HIPAA-compliant Authorization or Release of Information.

When in doubt, document the disclosure.

C. Individuals should be encouraged to put requests in writing for an accounting of disclosures but this cannot be required. Retain all written requests for an accounting. Requests may extend back up to six (6) years. Accountings must be provided within sixty (60) calendar days of the request. The Covered Component may grant itself one thirty (30) day extension if it does so within the original sixty (60) calendar days and provides the Individual with a written explanation.

D. The disclosure documentation and the accounting (not for research) each must include:

1. Date of disclosure,

2. Name and address of the entity or person that received the PHI,

3. A brief description of the PHI disclosed, and

4. A brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure.

For multiple disclosures to the same recipient, the accounting need only include:

1. The information listed above with respect to the first disclosure during the accounting period,

2. The frequency, or number of the disclosures made during the accounting period; and

3. The date of the last such disclosure during the accounting period.

E. Research Accounting Disclosure Documentation: If the Covered Component makes disclosures of PHI about 50 or more Individuals for research purposes that do not require an Authorization, the Covered Component may account for such disclosures by providing a requesting Individual with general information about the research for which the Individual's PHI may have been disclosed. The special accounting provided for high-volume (50 or more) research disclosures is called a Research Accounting and must include all of the following:

1. Name of the protocol or other research activity.

2. Description, in plain language, of the research protocol or other activity, including purpose and criteria for selecting Individual records.

3. Brief description of the type of PHI disclosed.

4. Date or period of time during which disclosures occurred, including date of the last such disclosure during the accounting period.

5. Name, address, telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

6. Statement that the PHI of the Individual may or may not have been disclosed for a particular protocol or research activity.

Note: Disclosures to the Secretary and for national security purposes have special rules governing accountings.

F. The Covered Component must temporarily suspend the Individual's right to an accounting of a disclosure to a health oversight or law enforcement agency, if the agency states that providing the accounting would be reasonably likely to impede the agency's activities.

1. If the statement is in writing, it must specify a time and that time must be honored.

2. If the statement is verbal, it must be documented and is valid for no longer than thirty (30) calendar days, unless a written statement specifying a longer time is received.

G. Fee for Accounting: The first accounting provided by a Covered Component to an Individual in any twelve (12) month period shall be provided without charge in connection with processing and producing the requested accounting. For each subsequent Request for an Accounting during such twelve (12) month period the Covered Component may charge the Individual a reasonable cost per page for copying.

H. Documentation: The Covered Component shall retain all Individual Requests for Accounting and Covered Component Responses to Requests (including summaries) in the Individual's permanent record for at least six (6) years.

6. PERSONAL REPRESENTATIVES

45 CFR 164.502(g)

A. Personal representatives have all of the rights of the Individual (*e.g.,* to a notice of privacy practices, right to access, and right to accounting of disclosures), but only within the scope of the authority held by the personal representative. For example, a person with a limited healthcare power of attorney to decide whether to provide life support has rights only to PHI relevant to that decision. Documentation of the authority is required.

B. For adults and emancipated minors, a personal representative is only a person who has documentation providing authority to make decisions regarding healthcare on behalf of the Individual.

C. For non-emancipated minors, state law determines if the personal representative is the parent, guardian, or other person legally standing in as the parent (legal custody).

1. State and federal law govern when PHI is required to be disclosed to the parent, may be disclosed or when access or disclosure is prohibited.

2. Unless otherwise provided by state law, a parent is not the personal representative of a minor for purposes of HIPAA when:

a. the minor is authorized by law to consent or obtain the healthcare services without another person's permission and has actually consented to or obtained the healthcare services without another person's permission.

b. someone else other than the personal representative, such as a court, authorized the healthcare services.

c. the parent has agreed to a confidential relationship between the minor and the provider.

3. If state law is silent on who has legal custody of a non-emancipated minor, disclosure is permissible only if approved by a licensed healthcare professional, in the exercise of professional judgment. 45 CFR 164.502(g)(3)(ii)(C)

D. Disclosure to any personal representative may be denied if there is:

1. Inadequate documentation, or

2. Reasonable belief that:

a. the Individual has been subjected to domestic violence, abuse, or neglect by the personal representative,

b. treating the person as the personal representative could endanger the Individual, or

c. in the exercise of professional judgment it would not be in the best interest of the Individual. All such decisions must be documented.

E. For deceased persons, the personal representative is the person authorized by state law to act on behalf of the deceased or the estate. After an Individual's death, disclosures can be made to those persons that demonstrated involvement in care or payment for care during the decedent's life and to whom the Individual never objected to the person's involvement during his or her life. Disclosures of PHI can also be made to a person able to present Letters

Testamentary or Letters of Appointment over the Individual's estate or to the person named in a small estate affidavit. If no documentation exists of appointment, follow ORS 192.573 "Personal representative of deceased Individual." A will is never sufficient to demonstrate personal representation to receive PHI of a decedent. *See Sec. 16.*

7. "MINIMUM NECESSARY" AND VERIFICATION STANDARDS

45 CFR 164.502(b), 45 CFR 164.514(d)

A. Workforce Members shall make reasonable efforts to avoid requesting, using, or disclosing an entire PHI file and shall only request, use, or disclose the minimum necessary PHI to legitimately accomplish the intended purpose of the request, use or disclosure.

1. This Minimum Necessary determination **is <u>not</u> required** for:

   a. Disclosure to or requests for PHI from a treatment provider, for treatment purposes. Minimum Necessary standards apply to <u>use</u> of PHI for treatment.
   b. Disclosure to the Individual who is the subject of the PHI (including the personal representative).
   c. Disclosure or use pursuant to a specific authorization from the Individual.
   d. Disclosure to the U.S. Department of Health and Human Services required under Section 4(R) for enforcement purposes.
   e. Disclosure, requests for or use of PHI mandated by other law (*e.g.*, reporting of neglect or abuse).
   f. Uses or disclosures required to comply with HIPAA.

2. Minimum Necessary standard **always governs requests** for, use and disclosure of PHI for:

   a. Payment or non-treatment related healthcare operations, including internal disclosures.
   b. Incidental Disclosures to other Covered Components within the County to carry out job duties.
   c. Permitted internal communications (e.g., treatment) regarding psychotherapy notes.
   d. Use/disclosure requests that have been restricted through an Individual's granted restriction request.

B. Rather than make their own minimum necessary determination, a Workforce Member may rely on an assurance from the following that they are requesting only the "minimum necessary" PHI:

1. A public official requesting PHI for a permitted disclosure.

2. Another covered entity.

3. A healthcare professional working for a Business Associate of the County, as long as it is for a permitted disclosure.

4. Researchers with appropriate authorization from the Institutional Review Board or Privacy Board.

C. Each Covered Component shall identify those Workforce Members or classes of Workforce Members who need access to PHI for business purposes, the category or categories of PHI to which access is needed and any conditions appropriate for such access. Each Covered Component shall adopt internal procedures to reasonably limit Workforce Member authority to request, use, and disclose PHI to those Workforce Members and categories of PHI so identified. Each Covered Component must educate Workforce Members that systems are for business purposes only and never for personal curiosities. Covered Components shall ensure that access to systems containing PHI are shut off when a Workforce Member's employment or service terminates or role changes.

D. Each Covered Component shall periodically monitor access of systems to ensure only appropriate Workforce Members have access to PHI.

E. Each Covered Component shall adopt internal procedures governing the routine requests for, uses, and disclosures of PHI reasonably necessary to carry out the responsibilities of the Covered Component. For each routine disclosure, the Covered Component needs to identify:

1. the types of PHI to be disclosed,

2. the recipients who may receive the PHI,

3. the conditions that would apply to such access, and

4. the standards for disclosures to routinely hired types of Business Associates.

F. Each Covered Component shall adopt internal procedures for identifying, considering, and deciding on non-routine requests to receive, use, or disclose PHI. These procedures at a minimum shall provide for review by the Covered Component's Privacy Manager to determine if the criteria for disclosure are met, to verify the identity and authority of the requester(s), if not known to a Workforce Member and to appropriately document all non-routine requests and disclosures. Only those portions of PHI that are justified under this review should be released.

G. Unless the Individual is present and able to object, no disclosure of PHI shall occur without first verifying the identity of the person and the basis for the person's entitlement (authority) to receive the PHI. Unless expressly provided otherwise, the Covered Component may in good faith rely on whatever verbal statements, documentation, or other information is provided and in the exercise of professional judgment is believed to be necessary under the circumstances. If it is reasonable under the circumstances, the identity and authority of a public official or a person acting on behalf of the public official may be verified by presentation of agency identification, badge, a request on agency letterhead, contract, or other written authorization. 45 CFR 164.420(h)

H. A use or disclosure that exceeds the minimum necessary standard must be reported as a potential breach of PHI.

I. When leaving a message with an Individual on voice mail, Covered Components shall implement procedures to ensure only a high level purpose of the call is disclosed. The Individual's permission to otherwise leave a more detailed message must be documented in the Individual's record.

8. ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

45 CFR 164.504(c)

HIPAA recognizes that certain Incidental Disclosures of PHI in the Covered Component are inevitable. They are not a violation if the Covered Component has adequate safeguards in place.

A. Each Covered Component shall adopt procedures to minimize disclosure of PHI, inadvertently or otherwise, to non-Covered Components of the County or anyone else except for permitted disclosures. Each Workforce Member will use due care in limiting Incidental Disclosures as much as is reasonably practicable and will use caution and professional judgment when handling or using PHI. Including, but not limited to:

1. Separately identify and maintain files containing PHI in secure areas; limit access to those having a permissible purpose; organize files to minimize risk of inadvertent disclosure of PHI components; disclosure authorizations or restrictions shall be readily visible.

2. Files containing PHI shall be clearly designated as such. No PHI shall be visible on the cover.

3. Files eligible to be destroyed shall be promptly shredded and destruction documented.

4. Verbal disclosures shall be done in such a way as to minimize the risk of others overhearing PHI. Enclosed offices, conference rooms, or other secure areas shall be used when feasible.

5. Computer screens containing PHI shall be positioned or shielded to minimize access and automatic screen savers shall be used. Computers with access to PHI shall be secured when not in use.

6. Use of emails to transmit PHI outside of the County shall be encrypted. Safeguards must be in place to prevent disclosure to unauthorized recipients. De-identify PHI when feasible.

7. Access to databases, emails, or other electronic information shall be restricted to those members of the Covered Component, Business Associates, providers, or others having a legitimate and permissible need for access.

8. Files or documents containing PHI shall be not be left unattended or on display when not in use.

9. For fax transmittals, confirm that the proper number has been dialed and that only the proper recipient will receive the fax. Ensure that PHI received by fax is accessible only to authorized Workforce Members and is dealt with promptly.

10. Covered Component functions and Workforce Members shall be physically segregated from non-Covered Components and Workforce Members to the extent feasible.

11. Adopt safeguards to help ensure that Workforce Members who perform both covered and non-covered functions adequately delineate and compartmentalize their work.

12. Securely transport PHI when outside the County. PHI shall not be left unattended in vehicles or in public locations.

13. Any paper containing PHI and eligible for destruction must be securely destroyed by disposing of it in locked shred bins and never disposed of in open recycling bins or in the trash.

B. No less than once each year, each Covered Component Privacy Manager shall conduct a self-assessment of use and disclosure risks and take such steps as are necessary to address risk areas. This assessment and a description of remedial steps shall be provided to the County Privacy Officer.

9. NOTICE OF PRIVACY PRACTICES

45 CFR 164.502(i), 45 CFR 164.520

A. Except for inmates, every Individual has a right to notice of:

1. The uses and disclosures of PHI that may be made by the Covered Component;

2. The Individual's rights regarding his or her PHI;

3. The Covered Component's legal duties with respect to PHI.

B. A Covered Component's Notice of Privacy Practices (NPP) must include:

1. The following statement as a header or otherwise prominently displayed: "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."

2. A description that includes sufficient detail to place the Individual on notice, including at least one example, of the types of uses and disclosures that the Covered Component is permitted to make for treatment, payment, and healthcare operations.

3. A description that includes sufficient detail to place the Individual on notice of each of the other purposes for which the Covered Component is permitted or required to use or disclose PHI without the Individual's written authorization.

4. A statement that other uses and disclosures will be made only with the Individual's written authorization and that the Individual may revoke such authorization as provided by 45 CFR § 164.508(b)(5).

5. Any specific prohibitions or material PHI restrictions imposed on the Covered Component by any other law.

6. A statement of the Individual's rights with respect to PHI and a brief description of how the Individual may exercise these rights, as follows:

   a. The right to request restrictions on certain uses and disclosures of PHI as provided by 45 CFR § 164.522(a), including a statement that the Covered Component is not required to agree to a requested restriction except in situations of self-pay;

   b. The right to receive confidential communications of PHI as provided by 45 CFR § 164.522(b), as applicable;

   c. The right to inspect and copy PHI as provided by 45 CFR § 164.524;

   d. The right to amend PHI as provided by 45 CFR § 164.526;

   e. The right to receive an accounting of disclosures of PHI as provided by 45 CFR § 164.528; and

   f. The right of an Individual, including an Individual who has agreed to receive the NPP electronically, to obtain a paper copy of the notice from the Covered Component upon request.

7. A statement that the Covered Component is required by law to maintain the privacy of PHI and to provide Individuals with notice of its legal duties and privacy practices with respect to PHI.

8. A statement that the Covered Component is required to abide by the terms of the NPP currently in effect.

9. For the Covered Component to apply a change in a privacy practice that is described in the NPP to PHI that the Covered Component created or received prior to issuing a revised NPP, in accordance with 45 CFR § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its NPP and to make the new NPP

provisions effective for all PHI that it maintains. The statement must also describe how it will provide Individuals with a revised NPP.

10. Contact information for the person (name or title) including telephone number designated at the Covered Component to receive Complaints or ask questions. The NPP must contain a statement that Individuals may complain to the Covered Component and to the Secretary if they believe their privacy rights have been violated, a brief description of how the Individual may file a Complaint with the Covered Component, and a statement that the Individual will not be retaliated against for filing a Complaint.

11. The date on which the NPP is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

C. The NPP promptly shall be modified to reflect any material change in the permissible uses, disclosures, Individual rights, the Covered Component's duties, or other privacy practices. A NPP may be modified substantively only with approval of County Counsel.

D. All Covered Components that have public access to workplaces shall post the NPP in a clear and prominent location stating that the complete NPP is available on request. Further, the NPP shall be posted on the County public website.

E. All Covered Components that have a direct treatment relationship with an Individual shall:

1. Provide the NPP directly to the Individual on the first day the service is provided. In an emergency treatment situation, this may be delayed until the first reasonably practicable opportunity after the emergency has ended.

2. Have extra copies for Individuals to take.

3. Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt and document any refusal.

4. Store such acknowledgement or refusal with the Individual's clinical record.

If the NPP is subsequently changed, revised copies must be made available in areas of public access but need not be directly provided and no new acknowledgment is required.

D. Electronic Notice:

1. Each Covered Component shall prominently post its NPP on its web site and make its NPP available electronically through the web site.

2. Each Covered Component can provide the NPP to an Individual by email, if the Individual agrees to electronic notice and such agreement has not been withdrawn. The Covered Component must retain confirmation of the transmission of the email. If the Covered Component knows that the email transmission has failed, a paper copy of the NPP shall be provided to the Individual.

3. The Individual who is the recipient of electronic notice may obtain a paper copy of the NPP from the Covered Component upon request.

E. A Covered Component acting as a Business Associate of another covered entity is not required to distribute the NPP when it holds a role as a Business Associate unless otherwise required by a covered entity.

F. A Covered Component shall document compliance with the NPP requirements by retaining a copy(ies) of their NPP(s) for a period of six (6) years from the date of creation, or the date when such NPP(s) was last in effect, whichever is later.

10. AUTHORIZATION TO USE OR DISCLOSE PHI

45 CFR 164.508

A. Use or disclosure of PHI may occur only if permitted in this Policy or authorized by the Individual (e.g., marketing disclosures require an authorization). Generally, an Individual (or a personal representative) may authorize any disclosure of his or her own PHI.

B. Treatment, payment, or eligibility for healthcare benefits cannot be conditioned on the Individual providing an authorization to disclose PHI, except that:

1. A health plan may require one prior to enrollment to make eligibility or risk determinations.

2. A Covered Component may condition the provision of research-related treatment.

3. A Covered Component may condition the provision of treatment if the sole purpose of the Individual's treatment is to provide health information to a third party (e.g., disclosure of results of mandated drug test to an Individual's employer.)

C. A valid authorization must be in plain language, signed and dated by (or on behalf of) the Individual and contain all of the elements listed below. It must be separate from all other forms such as the consent to treatment.

1. A description of the PHI to be used or disclosed that identifies the information in a meaningful fashion. If the Covered Component intends to use or disclose mental health, alcohol and drug, genetic, or HIV information, then the Individual must specifically authorize each of these disclosures by initialing the applicable space on the form.

2. The name or specific identification of the person(s) or class of persons authorized to make the use or disclosure.

3. The name or specific identification of the person(s) or class of persons to whom the requested use or disclosure may be made.

4. A description of the purpose for the use or disclosure ("at the request of the Individual" is sufficient description if the Individual initiated the Authorization.)

5. An expiration date or expiration event, ("end of the research study" is sufficient if the Authorization is for a research-related use or disclosure.)

6. The signature and date of signature of the Individual whose information will be used or disclosed. (If a guardian or personal representative signs the Authorization, a description of the representative's authority to act for the Individual must also be provided.)

7. The Individual's right to revoke the Authorization in writing and either:

   a. exceptions to the right to revoke and a description of how the Individual may revoke the Authorization; or

   b. a reference to the Notice of Privacy Practices that may discuss exception to the right to revoke and a description of how an Individual may revoke an Authorization.

8. Either:

   a. a statement that the Covered Component may not condition treatment, payment, enrollment, or eligibility for benefits on whether the Individual signs the Authorization; or

   b. if the HIPAA Privacy Rule permits conditioning the provision of treatment, payment, enrollment, or eligibility for benefits on whether the Individual signs the Authorization, the consequences to the Individual of refusing to sign.

9. The potential for information disclosed pursuant to the Authorization to be redisclosed by the recipient and to no longer be protected by the HIPAA Privacy Rule.

D. An authorization may be revoked in writing at any time, but revocation does not affect uses or disclosures already taken in reliance on the authorization. An authorization is not valid if the Covered Component knows it has expired, has been revoked, or any material information is known to be false.

E. The original authorization is retained and a copy is provided to the Individual.

F. Psychotherapy notes require a separate authorization.

G. Certain conditions require a specific consent for disclosure such as genetic testing information and disclosures by programs subject to the federal substance abuse rules. The Individual must be given the following notice on the signed form when substance abuse information is being authorized for disclosure and the information is subject to 42 CFR Part 2:

   1. "This information may not be disclosed to anyone without the specific written authorization of the Individual to whom it pertains." (42 CFR 2.32)

2. "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal Rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal Rules restrict any of the information to criminally investigate or prosecute any alcohol or drug abuse patient." (42 CFR 3.32)

H. A Covered Component must obtain an authorization for any sale of PHI. Such authorization must state that the disclosure will result in remuneration to Columbia County.

I. Workforce Members must verify and document both the identity and authority of an Individual before disclosing information pursuant to an Authorization.

J. An Authorization form signed by the Individual does not give the named recipient the authority to act on behalf of the Individual, for example to consent to treatment. It only gives the authority for the Covered Component to disclose information to the recipient.

K. The Minimum Necessary Standard does not apply to disclosures pursuant to an Authorization.

11. RIGHT TO REQUEST A USE OR DISCLOSURE RESTRICTION / COMMUNICATIONS AT ALTERNATE LOCATIONS

45 CFR 164.502(c), 45 CFR 164.522(a)

A. Individuals, including inmates, must be given an opportunity to request that use or disclosure of PHI for treatment, payment, or healthcare operations or disclosure of PHI to friends and family members be restricted.

1. The request may be denied for any non-discriminatory reason except in one limited circumstance. Individuals may request that their PHI not be shared with a health plan when the Individual or someone on the Individual's behalf pays for the Individual's service in full and the use or disclosure is for payment or healthcare operations and not otherwise required by law. Such restriction request does not impact future disclosures made for the purpose of treatment.

2. If granted, the request must be honored, except:

   a. In case of medical emergency and, even then, the recipient of the information must be asked to not further use or disclose the PHI.

   b. Uses or disclosures of PHI to the Individual himself or herself.

   c. Uses or disclosures for any "public purpose" (*see* 45 CFR 164.512).

3. Agreement to restriction. Covered Components should only agree to such requests when exceptional circumstances exist, when the Covered Component can reasonably

accommodate the request, and when the Covered Component determines that the restriction can be maintained.

The agreement to restrict use and disclosure may be terminated if:

a. the Individual requests in writing (or verbally if documented in the Individual's record); or

b. the Covered Component terminates in writing; but the restriction remains in effect for previously received or created PHI.

4. Grant or denial of a restriction must be documented. The HIPAA Privacy Rule does not require a Covered Component to provide a reason for its denial. It also does not provide the Individual with a right to appeal a denial. The Covered Component should use professional judgment in determining how to provide notice of the denial to the Individual.

5. If the request is not explicitly denied, it is deemed accepted.

B. Reasonable requests to receive PHI communications by specified confidential alternate means or to a specified alternate location must be accommodated if:

1. Made in writing;

2. The Individual provides reasonable information about how payment, if applicable, for services rendered will be handled; and 45 CFR 164.502(h). 45 CFR 164.522(b)

3. The Individual has specified an alternative address or other method of contact.

C. Covered Component providers may not ask for a reason for a request to receive PHI communications by specified confidential alternate means or to a specified alternate location. However, health plans may require that the request contain a statement that disclosure of all or part of the information to which the request pertains may endanger the Individual.

D. Covered Components must notify the Individual not later than thirty (30) calendar days of receipt of request whether the request has been accepted or denied. If accepted, the Covered Component must:

1. ensure Business Associates are aware of alternate contact information;

2. inform all appropriate Workforce Members who may communicate with the Individual of the accommodation, including but not limited to, the Individual's County case manager, quality management staff, and business services staff; and

3. ensure that all relevant computer electronic records or files are flagged or marked to reflect any approved accommodation including updates to addresses and phone numbers. This includes providing a note to link with the original request housed in the Individual's permanent record or other method for ensuring that electronic files, if

communicated or released to the Individual, are done so according to the Individual's request.

12. RIGHT OF INDIVIDUAL TO ACCESS PHI

45 CFR 164.502(a), 45 CFR 164.524

A. An individual has a right to access, inspect, and copy his or her own PHI held in the Designated Record Set except:

1. Psychotherapy notes.

2. PHI compiled for use in or reasonable anticipation of a criminal, civil, or administrative proceeding.

3. An inmate's right to copy PHI (but not the right to inspect) may be denied, if copying would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or others in the facility or those responsible for transporting the inmate.

4. If the PHI were permissibly obtained in confidence from someone other than a healthcare provider and disclosure would be reasonably likely to reveal the source of the information.

5. Certain federal law grounds. These grounds for denial are not subject to review under HIPAA.

6. If the requested information has been obtained by the Covered Component in the course of research that includes treatment of the research participants, the Individual's right to access this information may be temporarily suspended for as long as the research is in progress; provided that: a) the Individual has agreed to the denial of access when consenting to participate in the research that includes treatment; and b) the Covered Component has informed the Individual that his or her right to access the information will be reinstated once the research is completed.

B. The request for access must be made in writing.

C. Types of Action on a Request: The Covered Component may take one of the following actions on a request.

1. Determine that the Individual has no right to access and deny the request without an opportunity to review as set forth above in paragraph A, above.

2. Deny the Request and give the Individual an opportunity to obtain a review of the denial as set forth below in paragraph D, or

3. Provide access as described below in paragraph E.

D. The right to access may be denied on the following grounds, if the Individual is given a right to review the denial and a licensed healthcare professional determines that:

1. Access would be reasonably likely to endanger the life or physical safety of the Individual or another person,

2. Another person (other than a healthcare provider) is mentioned in the PHI and access would likely cause substantial harm to that person, or

3. A request from a personal representative likely would result in substantial harm to the Individual or another person.

E. A request for access must be acted on within thirty (30) calendar days. Covered Components that have programs under the jurisdiction of ORS 179.505 must respond within five (5) working days. Respond as follows:

1. Grant, in whole or in part, by providing access to, or mailing a copy of the PHI, in the form or format requested if readily producible or, if not, by hard copy. If the same PHI is in multiple locations, only one access point or copy need be provided. Copies of records may be provided to an Individual or a third party that the Individual identifies in an electronic or paper format depending on the Individual's request and the technology in which the records are maintained. Any electronic delivery of PHI must be encrypted.

   a. A summary may be provided if agreed to in advance by the Individual. If the Individual requests a summary of the PHI requested, in lieu of providing an opportunity to inspect or obtain a copy of the full Designated Record Set, the Individual must agree in advance to any provisions of the summary, any fees imposed by the Covered Component for such summary and to any extended time needed by the Covered Component to produce the summary.

   b. If the Covered Component approves the request and would like to provide an explanation to accompany the information being released to the Individual, the Covered Component may do so, but only if the Individual agrees in advance to any provisions of the explanation and to any fees imposed by the Covered Component for such documents.

2. Deny, in whole or in part, by sending notice in writing and containing:

   a. The basis for denial;
   b. A description of any applicable review rights; and
   c. A description of the Complaint procedures.

   If the Covered Component denies access in whole or in part as outlined above, the Covered Component shall, to the extent possible, give the Individual access to any other information requested after excluding the PHI to which the Covered Component had grounds to deny access.

3. If the Covered Component does not have the PHI requested, inform the Individual of where to direct his or her request, if known. The obligation to provide access extends to PHI held by the Covered Component's Business Associates.

F. If a review of a denial is requested, it must be done by a licensed healthcare professional designated by the Covered Component, who was not involved in the initial denial. This professional's decision is final and binding.

G. The responsibility to provide access extends not only to PHI in its own possession, but also to PHI that is a Designated Record Set of its Business Associate. Workforce Members must check with any applicable Business Associate about information held by it when fulfilling requests. The Covered Component may ask the Business Associate to provide access to the Individual directly.

H. Copies of records may be provided to an Individual or a third party that the Individual identifies in an electronic or paper format depending on the request and the technology in which the records are maintained. The third party must be designated in writing by the Individual. Any electronic delivery of PHI must be encrypted.

I. Fees:

1. Categories of Fees: A Covered Component may charge a requesting Individual the following reasonable, cost-based fees associated with obtaining access to his or her PHI, but may not deny access due to inability to pay fees associated with access. Any fees collected by the Covered Component shall be recorded as revenue to that Covered Component.

   a. Copying: Fees may include the labor and supply costs (for electronic or paper form);
   b. Mailing: Fees may include copying costs and the cost of postage;
   c. Electronic: Fees may include the cost of a portable media storage device, e.g., flash drive.

2. No Handling Fees: The Covered Component shall not charge any fees for retrieving or handling information or for processing the request.

3. Preparation of Summary or Explanation: The Covered Component may charge by the hour for the preparation of an explanation or summary of the information requested by the Individual, if:

   a. the Individual requests such explanation; and
   b. the Individual agrees to the fees in advance of the preparation.

J. Documentation for Communication with Individuals: The Covered Component shall maintain all written communications to or from an Individual regarding his or her right to access PHI in the medical record for the Individual. All documentation associated with requests shall be retained for at least six (6) years from the last date of service, the termination of any litigation or audit involving the record whichever is later.

13. RIGHT OF INDIVIDUAL TO REQUEST AMENDMENT OF PHI

A. An Individual may make written request that PHI held in the Designated Record Set be amended, stating the reasons for the request.

B. Determinations of whether to accept or deny the request for an amendment will be made by the Covered Component following a review of the relevant record and Designated Record Set, consultation with the treating physician or clinical manager, evaluation of the request, and to the extent appropriate, other health professionals familiar with the Individual's course of treatment.

C. A request to amend must be acted upon within sixty (60) calendar days by:

1. Granting the request in whole or in part by:

a. identifying the records in the Designated Record Set that are affected by the amendment;

b. at a minimum, appending the record or providing a link to the amendment;

c. informing the Individual; and

d. making reasonable efforts to provide the amendment within a reasonable time to persons identified by the Individual and any other person known to have the information who may have relied, or reasonably could rely, on the information (including Business Associates).

2. Denying the request in whole or in part in writing, providing:

a. the basis for denial using plain language (*See* paragraph C below);

b. how to file a Complaint with the Covered Component or the Secretary;

c. information on how to submit a written statement disagreeing with the denial; and

d. a statement that, if the Individual does not submit a statement of disagreement, the Individual may request that the Covered Component provide the Individual's request for amendment and the denial with any future disclosures of the PHI that may be the subject of such disclosure.

3. Extending the timeframe for responding to the request, by:

a. providing the Individual with a written statement of the reasons for the delay; and

b. the date by which the Covered Component will complete its action on the request (which cannot be later than thirty (30) calendar days).

Only one extension is allowed.

D. The grounds for denial are that the PHI or record:

1. Was not created by the Covered Component unless the Individual provides a reasonable basis to believe that the person who created the PHI is no longer available to act on the requested amendment;

2. Is not held by the Covered Component in the Designated Record Set;

3. Is PHI that the Individual does not have a right to inspect, e.g., psychotherapy notes, information prepared for criminal, civil or administrative proceedings; or

4. Is already accurate and complete.

E. If the request is denied, the request for amendment, denial, statement of disagreement, and any rebuttal created by the Covered Component must be appended or linked to the PHI. These must be included with any subsequent disclosure. Special rules apply to electronic standard transaction codes.

F. The Covered Component may reasonably limit the length of a statement of disagreement. The Covered Component may choose to prepare a written rebuttal to the Individual's statement of disagreement. Whenever such a rebuttal is prepared, the Covered Component shall provide a copy to the Individual within thirty (30) calendar days of receiving the statement of disagreement.

G. If the Covered Component receives an amendment from another covered entity, it also must append or link the amendment to the PHI.

H. Each Covered Component must document the name and title of all persons authorized to review and decide on amendment requests. Such information must be retained for at least six (6) years.

I. Documentation: The Covered Component shall retain all documentation associated with requests for amendments (and all associated determinations) for the longer of six (6) years from the date of the last service in the record, termination of litigation or an audit involving the record.

14. COMPLAINTS

A. Each Covered Component's Privacy Manager is responsible for receiving and addressing Complaints regarding violations of this Policy, the Covered Component's specific procedures, or HIPAA.

B. At the time of receipt, a complainant shall be informed that:

1. Complainant is encouraged, but not required to put the Complaint in writing;

2. Complainant has the option of filing the Complaint with the County Privacy Officer. The Complaint shall be filed directly with the County Privacy Officer, if it involves the person responsible for receiving Complaints;

3. That Complainant may bypass the County Complaint process and file the Complaint directly with the Secretary; and

4. That the law and County policy prohibit retaliation against any Complainant.

C. The Workforce Member receiving the Complaint shall document:

1. The name and contact information for the Complainant;

2. The specific nature of the Complaint, including sufficient information to investigate and address the Complaint; and

3. That the information described above was provided.

D. The Privacy Manager receiving the forwarded Complaint shall route the Complaint to the appropriate person to investigate the circumstances and either deny the Complaint or take such actions as are reasonably necessary to address the Complaint, including but not limited to mitigating any adverse impacts of an impermissible request for, use of, or disclosure of PHI. If the person receiving the Complaint does not have authority to resolve the matter, the person shall make a recommendation to an appropriate manager. The resolution of the Complaint, including any changes in policies or procedures and any actions taken in response to the Complaint must be documented.

E. Complaints should be addressed within thirty (30) calendar days of receipt. The County Privacy Officer shall be provided the information described in paragraph C no later than thirty (30) calendar days after receipt of the Complaint. In the event the Complaint was denied or the Complainant is not satisfied with the resolution, the County Privacy Officer shall review the matter and determine whether the action taken was appropriate and may implement an alternate course of action. The Complainant shall be informed of any County Privacy Officer decision in writing within thirty (30) days of receipt.

F. Any initial Complaint that results in Breach must be handled in accordance with *Sec. 25.*

Note: Whistleblower Protection.

State law affords certain protections to "whistleblowers." This may require that the Complainant's identification be kept confidential. The person receiving the Complaint shall promptly notify County Counsel if, due to the nature of the Complaint, statements from the Complainant or for any other reason, the person thinks the Complainant may qualify as a "whistleblower."

15. INMATES

A. Inmates are adults or juveniles in custody in a prison, jail, correctional center, halfway house, or similar facility. Persons released from the facility, including on parole or probation are not inmates and no longer in custody and their PHI is treated as that of any other Individual.

B. Inmate PHI is handled differently as follows:

1. A Covered Component may disclose PHI about an inmate to any correctional facility or law enforcement official having custody over the inmate, provided that the facility or official represents that the PHI is necessary for:

a. Providing healthcare to the inmate.
b. The health and safety of the inmate or other inmates.
c. The health and safety of employees or others at the facility.
d. The health and safety of persons transporting inmates.
e. The needs of law enforcement at the facility.
f. Administration and maintenance of safety, security, and good order at the facility.

2. Inmates do not have a right to a Notice of Privacy Practices and correctional facilities do not need to post one.

16. DECEDENTS

45 CFR 164.502(f), 45 CFR 164.512(g) and (h)

A. Generally, protection of PHI survives 50 years after an Individual's death.

B. In addition to the other permissible disclosures listed above, it is permissible to disclose PHI about a decedent to:

1. Coroners and medical examiners to identify a deceased person, determine cause of death, or other purpose authorized by law. The medical examiner may only use or disclose PHI as permitted in these guidelines.

2. Funeral directors as necessary to assist them in carrying out their duties. This may be prior to, and in reasonable anticipation of, death.

3. To organ procurement organizations to facilitate transplant donations. This permission does not allow disclosures in connection with live donor activities. In live donor situations, an authorization is required.

4. Law enforcement to alert of possible criminal conduct.

17. PSYCHOTHERAPY NOTES

45 CFR 164.508(a)(2)

A. Psychotherapy notes include notes of a mental healthcare professional documenting or analyzing the contents of a conversation during a private, joint, group, or family counseling session that are separated from the Individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, session start/stop times, modalities and frequencies of treatment, results of clinical tests and any summary of a diagnosis, functional status, treatment plan, symptoms, prognosis, or progress to date.

B. Requests for, use, and disclosure of psychotherapy notes must be documented and are permitted only with a separate written authorization of the Individual, <u>except</u>:

1. Use for treatment purposes by the mental health professional that created the notes.

2. Use by the Covered Component for supervised internal training to improve counseling skills.

3. To defend against a legal action brought by the Individual.

4. To make a use or disclosure that is required by a law, complies with such law and is limited to the relevant requirements of such law.

5. When required as part of oversight of the practitioner.

6. To make a use or disclosure to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by Oregon law.

7. To make a use or disclosure that is consistent with law and the standards of ethical conduct, if the Covered Component, 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 and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.

8. When required by the Secretary to investigate or determine the County's compliance with HIPAA.

C. Individuals do not have a right to access their own psychotherapy notes. Such access may be denied for any legitimate reason. Further, for Covered Components that have programs under the jurisdiction of ORS 179.505, the Individual does not have a right to challenge any such denial. ORS 179.505(9)(b).

D. Psychotherapy notes must be kept separate from the medical record. Psychotherapy notes lose protection as such if they are co-mingled with the medical record.

18. MARKETING

45 CFR 164.501 and 45 CFR 164.508(a)(3)

The County may communicate with an Individual face-to-face about products or services that may interest the Individual or give an Individual a promotional gift of nominal value. Otherwise, the County does not use or disclose an Individual's PHI for marketing without the Individual's authorization.

19. FUNDRAISING

45 CFR 164.514(f)

The County may not use PHI for fundraising communications, as defined under HIPAA.

20. USES AND DISCLOSURES OF PHI CREATED FOR RESEARCH

45 CFR 164.512(i)

The County may use or disclose limited PHI for research to the extent allowed by HIPAA and state law. The County shall obtain the Individual's authorization for use or disclosure of PHI for research purposes or obtain a waiver of the authorization requirements from an Institutional Review Board (IRB) or Privacy Board, including a Privacy Board chaired by the County Privacy Officer, after deliberation and consideration of criteria.

Covered Component business functions do not necessarily include conducting research. If the need for research does arise, the County Privacy Officer and County Counsel must be notified.

A. Informed Consent: Informed consent enables each Individual to voluntarily decide whether or not to participate as a research subject. An informed consent is documented by the use of a written consent form approved by an institutional review board (IRB) and signed by the Individual. Such consent form will be provided to a subject in written form prior to such subject's participation unless a waiver of informed consent is approved by an IRB.

B. Authorization: In addition to informed consent, an authorization must be obtained from the Individual unless an IRB or Privacy Board approves a waiver of authorization, the information is De-Identified, or the PHI is disclosed in a Limited Data Set pursuant to a data use agreement.

C. Waiver of Informed Consent and/or Authorization: When relying on a waiver of authorization or alteration of the informed consent, the IRB must document the following:

1. A statement identifying and confirming the authority of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved.

2. A statement that the IRB or Privacy Board has determined that the alteration or waiver satisfies the following criteria:

    a. the use or disclosure of PHI involves no more than minimal risk to the Individual's privacy;
    b. the research could not practicably be conducted without the alteration or waiver; and
    c. the research could not practicably be conducted without access to and use of the PHI.

3. At least the following elements must be present to ensure that there is a minimal risk to the Individual's privacy:

    a. an adequate plan to protect the identifiers from improper use or disclosure;

    b. an adequate plan to destroy the identifiers at the earliest possible opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or their retention is required by law; and c. adequate written assurances that the PHI will not be used or disclosed to any other person, except as required by law, for authorized oversight of the

research study, or for other research for which use or disclosure of the PHI would be permitted under the Privacy Rule.

4. The documentation must include a brief description of the PHI for which use or access is necessary, as determined by the IRB or Privacy Board.

5. The documentation must include a statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures.

6. The chair of the IRB or Privacy Board, or another member designated by the chair, must sign the documentation of the alteration or waiver of authorization.

21. DE-IDENTIFIED HEALTH INFORMATION

45 CFR 164.502(d), 45 CFR 164.514(a) and (b)

A. Health information that has been de-identified, *i.e.,* does not identify an Individual, nor provide a reasonable basis to identify an Individual, is not considered PHI. Covered Components may use PHI to create de-identified health information.

B. Covered Components may determine that health information is de-identified only if:

1. the Covered Component has designated the person as meeting the qualifications specified in 45 CFR 164.514(b)(1) and that person applies the standards set forth therein to the information, or

2. the following identifiers of the Individual or of relatives, employers, or household members of the Individual, are removed as specified in 45 CFR 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 geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. All elements of dates (except year) for dates directly related to an Individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, 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/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 finger and voice prints;
q. Full face photographic images and any comparable images; and
r. Any other unique identifying number, characteristic, or code, except as permitted under HIPAA.

The Covered Component must also not have actual knowledge that the information could be used alone or in combination with other information to identify an Individual who is a subject of the information.

C. Covered Components may assign a code or other means of record identification to allow de-identified information to be re-identified by the Covered Component only if:

1. the code is not derived from or related to information about the Individual or otherwise capable of being translated so as to identify the Individual, and

2. the code is not used for any impermissible purpose or disclosed.

D. Covered Components will not use or disclose de-identified information about genetic testing unless the Covered Component notified the Individual when the genetic test information was obtained of the Individual's right to object to the use or disclosure of de-identified genetic test information, or unless the disclosure is otherwise authorized by law.

E. Third Parties. Any third parties receiving PHI for the purpose of de-identifying it must have a Business Associate Agreement in place.

F. Different than Limited Data Set: De-identified information is not PHI. A Limited Data Set is still PHI.

22. LIMITED DATA SET

45 CFR 164.514(e)

A. The County may use or disclose a limited data set only for research, public health or healthcare operations purposes. County must enter into a data use agreement with the limited

data set recipient. A limited data set is PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual:

1. Names
2. Postal address information, other than town or city, state, and zip code
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locations (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints
16. Full face photographic images and any comparable images

B. Covered Components may use or disclose PHI except for genetic test information (ORS 192.537(2)) for the purposes of research, public health, or healthcare operations. The following conditions must be met before creating a Limited Data Set:

1. Valid Purpose: The purpose(s) of the use or disclosure of the Limited Data Set is research, public health or healthcare operations; and

2. Data Use Agreement: The Covered Component has entered into a valid Limited Data Set use agreement (the "Data Use Agreement") with the data set recipient (the "Data User"). A Data Use Agreement between Covered Component and a Data User is valid only if it establishes:

    a. the permitted uses and disclosures of the Limited Data Set by the Data User are for research, public health and/or healthcare operations purposes.

    b. who is permitted to use or receive the Limited Data Set and provides that the Data User will:

        i. not use or further disclose the information contained in the Limited Data Set other than as permitted by the Data Use Agreement or as otherwise required by law;

        ii. use appropriate safeguards to prevent use or disclosure of the information contained in the Limited Data Set other than as provided for by the Data Use Agreement;

iii. report to Covered Component any use or disclosure of the information contained in the Limited Data Set, which is not provided for by its Data Use Agreement, of which it becomes aware;

iv. iv. ensure that any agents, including subcontractors, to whom it provides the Limited Data Set agree to the same restrictions and conditions that apply to the Data User with respect to such information; and

v. not Individually identify the information or contact the Individuals.

C. Permission to Create Limited Data Set: A Covered Component may use PHI to create a Limited Data Set or disclose PHI to a Business Associate to create a Limited Data Set, whether or not the Covered Component is going to use the Limited Data Set. A third party that receives PHI to create a Limited Data Set must also have a Business Associate Agreement in place with the third party.

D. Exception to Accounting Requirements: A Covered Component is not required to account for its disclosure of a Limited Data Set regarding an Individual's right to receive an accounting of certain types of disclosures of PHI.

E. Minimum Necessary Standard: A Covered Component must limit the information of the Limited Data Set disclosed pursuant to this policy to the minimum necessary information needed for research, public health, or healthcare operations purposes specified in the Data Use Agreement.

F. Different than De-identified Information: A Limited Data Set is still PHI. De-identified information is not PHI.

23. BUSINESS ASSOCIATES

A. Each Covered Component shall identify its Business Associates and ensure that all contracts entered include Business Associate provisions approved by County Counsel.

B. The requirement for a written Business Associate agreement with a third party still pertains to services that fall under direct pay and that otherwise do not require a prime contract.

C. PHI shall not be disclosed to a Business Associate except in accordance with this Policy and the terms of the Business Associate provisions.

D. The Covered Component Privacy Manager shall be informed promptly if there are reasonable grounds to think that the Business Associate is failing to abide by its responsibilities or is failing to cooperate with the Covered Component.

E. Examples of situations where a Business Associate agreement is not required include:

1. Disclosure to a treatment provider for treatment purposes.

2. A healthcare provider submitting a claim to a health plan for payment.

3. Incidental Disclosures to persons or organizations that do not use PHI in the ordinary course of work, *e.g.*, a janitorial service or remodeler—provided that the Covered Component has taken reasonable steps to minimize the risk of disclosure.

4. Conduits that receive PHI but only for a limited time, such as the US Postal Service, Fed Ex, couriers.

5. Among covered entities participating in an organized healthcare arrangement (by IGA or contract).

6. From one governmental covered entity administering a public benefits program to another governmental covered entity administering a public benefits program serving the same or similar populations, to the extent necessary to coordinate or improve administration of the benefit programs.

7. With Workforce Members.

8. With entities receiving De-identified Information only.

F. Covered Component as a Business Associate to another covered entity.

1. The Covered Component is a Business Associate of another covered entity in situations where the Covered Component is acting on behalf of, or providing services to, another covered entity.

2. County Counsel must review any proposed Business Associate agreement by a covered entity that names the Covered Component, or County, as a Business Associate of another covered entity.

3. If the Covered Component subcontracts any of the services to a third party, the Covered Component must ensure that the subcontractor agreement includes a Business Associate agreement that is no less restrictive than the Covered Component's Business Associate agreement with the covered entity.

G. Covered Component as a subcontractor to a Business Associate of a covered entity.

1. The Covered Component is a subcontractor to a Business Associate of a covered entity in situations where the Covered Component is acting on behalf of, or providing services to, a Business Associate of another covered entity.

2. County Counsel must review any proposed Business Associate agreement by a covered entity that names the Covered Component, or County, as a subcontractor to a Business Associate of another covered entity.

24. MITIGATION / DUTY TO REPORT

45 CFR § 164.530(f)

The County will mitigate, to the extent practicable, any harmful effect that is known by the County to have occurred as a result of a use or disclosure of PHI in violation of the requirement of the HIPAA Privacy Rule or County policies and procedures by either the County or its Business Associates.

In cases of an impermissible disclosure by a subcontractor or Business Associate, either a treatment provider or non-covered entity, the Covered Component involved shall determine the mitigation plan. This may involve review of specific contract or agreement language regarding corrective measures or potential termination of a contract or agreement.

Workforce Members and Business Associates must immediately report known or suspected privacy or security Incidents or Complaints involving PHI to their Covered Component's Privacy Manager and/or County Privacy Officer. This includes a duty to self-report an Incident or Complaint caused by a Workforce Member.

The County will not tolerate retaliation against any Workforce Member who reports in good faith in accordance with this Policy or who participates in any investigation. The County will investigate reports of retaliation. Any Workforce Member who is an employee found to have engaged in retaliation may be subject to discipline, up to and including dismissal. Any Workforce Member who is not an employee found to have engaged in retaliation may be subject to termination of their services to the County. "Retaliation" does not include appropriate discipline or other sanctions imposed, when necessary, upon a Workforce Member who selfreports a possible violation.

Any Workforce Member who is an employee who fails to report known or suspected Incidents or Complaints as required by this policy may be subject to discipline. Any Workforce Member who is not an employee who fails to report known or suspected Incidents or Complaints as required by this policy may be subject to termination of their services to the County.

25. BREACH NOTIFICATION

45 CFR 164.400 et. seq.

Individuals have the right to be notified in the event that the County discovers a Breach of unsecured PHI.

Workforce Members are required to immediately report known or suspected privacy Incidents, Complaints and Breaches involving PHI to their Privacy Manager or the County Privacy Officer.

A. Investigation.

1. Upon receipt of a report, the Covered Component Privacy Manager in conjunction with the County Privacy Officer and County Security Officer, as applicable, shall

conduct an Investigation into the scope and cause. The internal Investigation will be completed within 30 calendar days of discovery by any Workforce Member.

a. Any barriers to the Investigation timeline shall be promptly raised to the County Privacy Officer or County Security Officer, as applicable.

b. Any ongoing harm to the Individual shall be mitigated or stopped as soon as reasonably possible.

c. A Workforce Member who unintentionally receives PHI should seek direction to delete or securely destroy the PHI without further using or disclosing it.

2. Internal Initial Notification Workflow for Investigation

a. The minimum necessary information will be shared with others in a prompt manner to ensure that all decision makers have information necessary to provide assistance with the Investigation. The primary responsibility for notification is by the Privacy Manager.

i. The Human Resources Manager will be notified and Personnel Rules and labor agreements will be followed if the report involves an act or omission of a Workforce Member.

ii. County Security Officer will be notified if the report involves data, ePHI, or forensic support is needed.

iii. The Facilities Manager will be notified if the report involves physical access to a County building.

iv. County Counsel's Office will be notified if report involves a threat of lawsuit or notification to individual's attorney or State Attorney General's office.

v. If the County is a Business Associate in the relationship with a third party Covered Entity, the County will notify the Covered Entity according to the Business Associate Agreement terms and follow direction by the Covered Entity.

vi. Managers, supervisors or Workforce Members of Covered Component where a report arose will be consulted for operational assistance for investigation and mitigation.

b. Sanctions.

i. If the report is related to an act or omission of a Workforce Member employee, the Privacy Manager will notify the Human Resources Manager and the Workforce Member's manager/supervisor.

ii. The Privacy Manager may choose to not request further involvement by the Human Resources Department when each of the following is supported by clearly documented facts for the event:

(a) The event is an unintentional act or omission by the Workforce Member,
(b) The event does not involve a reckless disregard of the Workforce Member's obligations in the sole discretion of the Privacy Manage,
(c) The event is the Workforce Member's first occurrence of any type involving PHI or ePHI,
(d) Privacy Manager does not need to gather any facts about the report from the Workforce Member(s) possibly implicated or implicated in the report.
(e) The supervisor/manager has already counseled the Workforce Member concerning way to reduce the risk of reoccurrence and address the event which involves reminders or training/education that the Privacy Manager believes is reasonable and appropriate to reduce the risk of reoccurrence, address the policy violation, and comply with breach notification requirements.

iii. Additional Human Resources Involvement

(a) Privacy Manager will request further assistance from the Human Resources Department when the criterion above is not met.
(b) Human Resources may consider other documented performance issues when determining the sanctions under this procedure.
(c) Considering the sanction factors listed below, Human Resources and the Privacy Manager will determine a category and sanction. The assigned sanction or corrective action will follow as part of the mitigation and remediation of the event.

Sanction Factors:
1. Knowledge of responsibilities
2. Cooperation with investigation
3. Type of PHI disclosed/sensitivity of information
4. Severity of resulting impact to County (media notifications and/or disclosure to Office for Civil Rights)
5. Repeated errors of same type
6. Mistake vs. intent

Categories:
1. Unintentional (mistakes or carelessness)
2. Reckless disregard (understanding obligation and failing to comply)
3. Intentional [Knowingly accessing/disclosing without a business need (*i.e.*, curiosity), for personal/financial gain, or to harm an Individual]

Sanctions for the category assigned may include any of the following:

1. Reminders
2. Training or education
3. Counseling
4. Verbal and/or written reprimand
5. Suspension
6. Reassignment (which may include termination of access to PHI)
7. Demotion
8. Termination

B. Breach Response Procedure.

1. The presumption is that a report of an unpermitted use or disclosure of Unsecured PHI is a Breach requiring notification to Individuals impacted.

   a. To demonstrate that notification is not required to Individuals impacted, the Investigation must include documentation of a risk assessment and approval by the County Privacy Officer resulting in either:

      i. a determination of a low probability the Unsecured PHI was compromised, or
      ii. an exception to the definition of a Breach.

   b. If Breach notification is required (or there is no risk assessment conducted that demonstrates a low probability the Unsecured PHI was compromised):

      i. The Privacy Manager in conjunction with Covered Component leadership, and the County Privacy Officer, shall develop a Breach notification letter (Notice) following the guidelines provided by the County Privacy Officer.

         (a) The Notice must be sent to each Individual (or parent/guardian if a minor child or other Personal Representative) whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of Breach.

         (b) Notice shall be given to the Individual's address of record unless an alternate address has been provided in an Individual Rights request. In such event, Notice shall be sent to the alternate address.

         (c) If Individual has requested no written communications, the Individual shall be contacted by phone and provided instructions on how to pick up the written Notice.

      ii. A leader from the Covered Component which has the relationship with the individual(s) impacted by the Breach shall sign the Notice. If the Breach impacts Individuals served by multiple departments, the Privacy Officer shall either sign the Notice or direct which countywide leader shall sign the Notice.

iii. In cases deemed to require urgency because ofpossible imminent misuse of Unsecured PHI, Notice by telephone or other means may be made, in addition to written Notice. However, verbal notice is not a substitute for written Notice.

iv. Deceased Individuals: If the Covered Component knows that some of the affected Individuals are deceased and knows the address of the next of kin or Personal Representative of the deceased Individuals, the Notice must be provided to the next of kin or Personal Representative.

v. Timing: The Notice must be sent by first class mail without unreasonable delay but no later than 60 calendar days after the date the Breach was discovered (or could have been discovered) unless a delay is requested by law enforcement. If law enforcement requests a delay, immediately notify the County Privacy Officer.

vi. Substitute notice. If the Covered Component has insufficient contact information for some or all of the affected Individuals, or if some Notices are returned as undeliverable, a substitute Notice must be provided for the unreachable Individuals. The substitute Notice should be provided as soon as reasonably possible after the Covered Component is aware that it has insufficient or out-of-date contact information for one or more affected Individuals. The substitute Notice must be reasonably calculated to reach the Individuals for whom it is being provided.

(a) If there are fewer than 10 Individuals for whom the Covered Component has insufficient or out-of-date contact information to provide the written Notice, the Covered Component may provide substitute Notice to such Individuals through an alternative form of written Notice such as secure e-mail, telephone or other means. Alternatively, posting Notice for at least 90 calendar days on the County's website home page may be appropriate if the Covered Component lacks any current contact information for the Individual(s).

(b) If the Covered Component has insufficient or out-of-date contact information for 10 or more Individuals, then the Covered Component must provide substitute notice through either a conspicuous posting for a period of 90 calendar days on the home page of the County website or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside.

(i.) Substitute Notice through the website or media for 10 or more Individuals requires the Covered Component to provide a toll-free phone number, active for 90 calendar days, where an Individual's Unsecured PHI may be included in the Breach.

(ii.) The Covered Component may attempt to cure out-of-date contact information of Individuals when Notices are returned as undeliverable by the United State Postal Service to avoid substitute notice so long as the Covered Component does so promptly upon receiving the returned notices and no later than 60 calendar days from discovery of the Breach.

(c) If the Breach affected more than 500 Individuals, the Notice must also be provided to prominent media outlets serving the County in the form of a press release, and the County Privacy Officer will simultaneously notify the Secretary, as set forth below.

C. Tracking. The Privacy Manager must thoroughly track the Investigation and document all pertinent information, communication, risk assessment (when required), notification and copies of supporting documentation in accordance with document retention requirements and in a tracking system as required by the County Privacy Officer. The Privacy Manager assigned to the event must actively monitor cases to ensure that all information tracked is kept current and accurate and cases do not become overdue or include inaccurate information.

D. Breach Notification to the Secretary of Health and Human Services or its designee.

1. All Breaches of Unsecured PHI must be reported in the manner specified on the U.S. Department of Health and Human Services website (HHS.gov).

   a. For Breaches affecting 500 or more Individuals, the report must be made immediately (concurrent with the notification sent to the Individuals).

   b. For Breaches affecting less than 500 Individuals, a log of such Breaches must be maintained and submitted annually no later than 60 calendar days after the end of each calendar year.

   c. If the County is considered a Business Associate to another Covered Entity in the relationship, the County will notify HHS or its designee as directed by the Covered Entity.

2. The County Privacy Officer reports Breaches of ePHI on behalf of the County Security Officer. The County Security Officer is responsible for ensuring the accuracy of submissions for any reportable Breach of ePHI before submission to the Secretary.

3. Breach reports will be resubmitted to the Secretary with updates as new information becomes available.

26. NO RETALIATION / NO WAIVER OF RIGHTS

45 CFR 164.430(g) and (h)

A. No Workforce Member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any Individual for exercising any right or participating in any process under this Policy, including filing a Complaint or reporting a known or suspected Incident or Breach in good faith;

2. Any Individual or other person for filing a Complaint with the Secretary, testifying, assisting, or participating in an investigation or compliance review, proceeding, or hearing; or

3. Any Individual or other person opposing any act or practice that unlawfully violates this Policy provided that it is based on a good faith belief that the act or practice is unlawful, the manner of opposition is reasonable, and does not involve the impermissible disclosure of PHI.

B. No Individual shall be required to waive his or her rights provided by HIPAA, 45 CFR 160.306, or 45 CFR part 164 as a condition of providing treatment, payment, enrollment in a health plan, or eligibility for benefits.

27. SANCTIONS

45 CFR 164.530(c)

A. Failure to comply with this Policy, or the implementing procedures, shall be grounds for discipline, up to and including termination. Any such discipline shall be documented and may be disclosed to the Secretary. Consideration will be given to:

1. Factors:

   a. Knowledge of responsibilities
   b. Cooperation with investigation
   c. Type of PHI disclosed/sensitivity of information
   d. Severity of resulting impact to County (media notifications and/or disclosure to the Office for Civil Rights)
   e. Repeated errors of the same type
   f. Mistake vs. intent

2. Categories:

   a. Unintentional (mistakes or carelessness)
   b. Reckless disregard (understanding obligation and failing to comply)
   c. Intentional, i.e., knowingly accessing/disclosing without a business need, for example, for curiosity, for personal/financial gain, or to harm an Individual

3. Sanctions for the category assigned may include any of the following:

   a. Reminders

b. Training or education
c. Counseling
d. Verbal and/or written reprimand
e. Suspension
f. Reassignment (termination of access to PHI)
g. Demotion
h. Termination

B. No employee shall be disciplined for disclosing information that the employee believes in good faith to constitute evidence that a Covered Component has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the Covered Component potentially endangers one or more Individuals, workers, or the public, provided that the disclosure is to:

1. a healthcare oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Covered Component or to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the Covered Component, or

2. an attorney retained by or on behalf of a person for the purpose of determining the legal options of the person with regard to the alleged improper conduct.

C. No employee, who is the victim of a criminal act, shall be disciplined for disclosing PHI to a law enforcement official provided that the PHI:

1. is about the suspected perpetrator of the criminal act; and

2. is limited to: name and address, date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment or death; and a description of distinguishing physical characteristics such as height, weight, gender, race, scars, tattoos. This does not include DNA, dental records, samples or analysis of body fluids or tissue. 45 CFR 164.502(j), 45 CFR 164.512(f)(2)

D. Workforce Members who are not employees of the County may also be sanctioned pursuant to this section up to and including termination of their service to the County.

28. AMENDMENTS TO POLICIES AND PROCEDURES

45 CFR 164.530(i)

A. This Policy, implementing procedures and all forms, shall be promptly revised to reflect changes in the law. Also, each Covered Component must review its HIPAA procedures at least once every 2 years and make changes as necessary to ensure compliance with HIPAA requirements.

B. This Policy may be amended only by the Board of Commissioners, upon recommendation of the County Administrator who must first consult with the County Privacy Officer and County

Counsel. A Covered Component's Privacy Manager must approve amendments to the Covered Component's implementing privacy procedures and practices.

C. Amendments that do not materially affect a privacy practice described in the Notice of Privacy Practices may be made at any time, but cannot go into effect until put into writing.

D. Amendments that materially affect a privacy practice described in the Notice of Privacy Practices:

1. Shall specify whether the change applies to information created or received prior to the change.

2. May only be implemented after the Notice of Privacy Practices has been revised and published.

E. Workforce Members must be notified of material changes to this Policy or any Covered Component procedures within a reasonable time of such changes.

29. DOCUMENT RETENTION

45 CFR 164.530(j)

A copy of all policies, procedures, forms, accounting of disclosures, Incidents, Breaches, Complaints and responses, use/disclosure authorizations and restrictions and all other items required to be documented under this Policy shall be retained for six (6) years, or the period specified in the State Archival rules, whichever is *longer.*

ATTACHMENT A

County Covered Components and Business Associates under HIPAA

The following County Departments are **Covered Components** under HIPAA:

- Community Justice
- Public Health
- Sheriff's Office (Corrections Division only)

The following Departments are **Business Associates** that perform work on the behalf of the Covered Components:

- County Counsel
- Finance
- Human Resources
- Information Technology