



OREGON YOUTH AUTHORITY

Policy Statement

Part I – Administrative Services



Subject:

Targeted Case Management - HIPAA Privacy and Security

Section – Policy Number:

E: Information Management – 3.5

Supersedes:

N/A

Effective Date:

10/29/2026

Date of Last

Review/Revision:

None

Related Standards and References:

- [45 CFR Part 160](#) General Administrative Requirements
- [45 CFR Part 164](#) Security and Privacy
- [OAR 413-050-0600](#) through 0670 (Targeted Case Management)
- [Oregon Cyber Disruption Response & Recovery - Voluntary Resource Guide for Local Government](#)
- [OYA policy: 0-7.0](#) Use of Electronic Information Assets and Systems
 - I-C-9.0 Mobile Communication Devices (Cell Phones) and Other Mobile Data Storage Devices
 - I-E-3.2 Information Asset Classification and Protection
 - I-E-3.3 Information Security Incident Response
 - II-F-1.1 Youth Grievance Process - Facility
 - III-A-2.0 Targeted Case Management
 - III-B-4.0 Youth Rights and Grievances in the Community
- OYA forms: [YA 3060](#) HIPAA Notice of Privacy Practices
- [YA 3060 SP](#) HIPAA Notice of Privacy Practices - Spanish
- [JJIS policy III-A-1](#) Granting Access to JJIS and JJIS Data

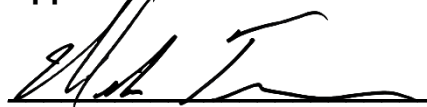
Related Procedures:

- [TS I-E-3.3](#) Service Desk Information Security Incident Response

Policy Owner:

Community Services Assistant
Director

Approved:


Mike Tessean, Director

I. PURPOSE:

This policy establishes requirements for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules. It designates OYA as a HIPAA hybrid covered entity and identifies the organizational components subject to HIPAA requirements (relating to Targeted Case Management).

II. POLICY DEFINITIONS:

Covered component: A designated organizational unit that performs functions subject to HIPAA requirements within a hybrid organizational entity.

Disclosure: The release, transfer, access or sharing of protected health information (PHI) with a person or entity outside of the TCM healthcare component.

Hybrid covered entity: A single legal entity that is a covered entity and whose business activities include both covered and non-covered functions, and that designates health care components in accordance with HIPAA Rule.

Juvenile Justice Information System (JJIS): An electronic information system developed and maintained by the state through OYA and administered in partnership with county juvenile departments.

Minimum necessary standard: The requirement to limit the use, disclosure or request of protected health information to the minimum amount needed to accomplish the intended purpose.

Personal representative: A person authorized under law to act on behalf of the individual in making health care related decisions.

Protected health information (PHI): Individually identifiable health information created, received, maintained or transmitted as part of OYA's designated health care component that relates to the provision of Targeted Case Management (TCM) services or payment for those services.

Release of information: A written authorization signed by the youth or their personal representative that permits the use or disclosure of protected health information for purposes not otherwise permitted by HIPAA.

Targeted Case Management (TCM): Activities performed by a JPPO to assist youth to obtain necessary medical, social, educational, counseling, or other services.

Treatment, Payment and Healthcare Operations (TPO): Activities permitted by HIPAA for which protected health information may be used or disclosed without youth authorization, when the information is needed to provide care, obtain payment for care, or support essential healthcare business operations.

III. POLICY:

OYA is designated as a HIPAA hybrid covered entity under 45 CFR § 164.103. Under this designation, only the portions of the agency that perform HIPAA covered functions are subject to the HIPAA Privacy, Security, and Breach Notification Rules.

The following functions are designated as covered components:

- Targeted Case Management (TCM) services billed to Medicaid;
- Juvenile parole/probation officers (JPPOs) responsible for providing and documenting TCM services;

- Field supervisors responsible for supervision and quality oversight of TCM services and documentation;
- Staff responsible for reviewing, submitting, or supporting TCM Medicaid billing transactions;
- Staff responsible for maintaining records used to support Medicaid claims for TCM services; and
- Information technology, fiscal, or administrative staff who support operations involving protected health information related to TCM services and billing.

IV. GENERAL STANDARDS:

A. Privacy Officer and Security Officer Designations

1. The HIPAA privacy officer is designated by the Community Services assistant director and is responsible for oversight and compliance with the HIPAA Privacy Rule, including:
 - a) Development and implementation of policy;
 - b) Workforce training;
 - c) Investigation of potential privacy violations;
 - d) Coordination of breach notifications;
 - e) Responding to privacy complaints; and
 - f) Ensuring appropriate use and disclosure of protected health information (PHI).
2. The HIPAA security officer is designated by the deputy director of administration and is responsible for oversight and compliance with the HIPAA Security Rule, including:
 - a) Implementation of administrative, technical and physical safeguards;
 - b) Protection of electronic PHI;
 - c) Monitoring system access and security risks; and
 - d) Security incident response coordination.

B. Notice of Privacy Practices

1. JPPOs must inform youth receiving TCM services of how their PHI may be used and disclosed and of their privacy rights under HIPAA by giving them a copy of the HIPAA Notice of Privacy Practices (NPP), OYA form YA 3060. The NPP must inform youth of:

- a) How their PHI may be used and disclosed;
 - b) OYA's legal duties to protect the privacy of their PHI;
 - c) The youth's rights regarding their PHI, including the right to access, request amendments and request restrictions; and
 - d) How to file a complaint regarding privacy practices.
2. JPPOs must provide the NPP to youth no later than the date of the first billable TCM service, and anytime youth request it. The NPP must be reviewed with youth in a manner that supports youth understanding, including reviewing key elements of the notice. JPPOs must:
- a) Bring two paper copies of the NPP to their initial contact with the youth;
 - b) Review the contents of the notice with the youth, including how to file a complaint;
 - c) Offer the youth a copy of the NPP or plain-language NPP FAQ to keep;
 - d) Make a good faith effort to obtain youth's signature on the NPP to acknowledge receipt and understanding; and
 - e) Document on the NPP if the youth refuses to sign, including the date of refusal and the JPPO's initials.
3. Staff must upload all NPPs (signed by youth or refused) to the youth's case file in JJIS under Imported Documents. Refusal to sign the NPP does not prevent the provision of TCM services or billing for those services.

C. Staff Handling of TCM PHI

1. TCM PHI is classified as Level 3 – Restricted Information in accordance with statewide policy and OYA policy I-E-3.2 Information Asset Classification and Protection. Staff must handle TCM PHI accordingly.
- In addition, staff must comply with all requirements of this policy when accessing, using or disclosing PHI. Staff who violate this policy or HIPAA requirements are subject to progressive discipline.
2. JPPOs, Financial Services staff, administrative staff, and designated data entry staff who work with TCM information are considered members of the TCM health care component and must follow the requirements of this policy when creating, accessing, reviewing, or transmitting TCM PHI.

3. Access to TCM PHI is limited to staff whose job duties involve providing, documenting, coordinating, overseeing or billing TCM services.
4. All OYA staff must complete HIPAA training prior to accessing JJIS and annually thereafter, regardless of their role. Training must include requirements related to the protection, access, use and disclosure of PHI, and staff responsibilities under this policy.
5. PHI may exist in electronic systems, printed documents, emails, or verbal communications. Staff members must protect PHI regardless of its format.
6. When handling TCM PHI, staff must:
 - a) Access PHI only when necessary to perform assigned job duties;
 - b) Protect PHI from unauthorized access, disclosure or misuse; and
 - c) Limit use and disclosure of PHI to the minimum necessary.
7. Handling PHI in Workspaces

Staff must ensure that PHI is not visible or accessible to individuals who are not authorized to view the information. When handling records containing PHI, staff must:

 - a) Ensure that screens and printed materials cannot be easily viewed by others;
 - b) Lock or log out of computers when leaving a workstation unattended; and
 - c) Avoid discussing PHI in areas where conversations may be overheard by unauthorized individuals.
8. Printed Records Containing PHI

Printed materials containing PHI must be protected from unauthorized access. Staff must:

 - a) Print PHI only when necessary to perform assigned duties;
 - b) Retrieve printed materials from printers immediately;
 - c) Store printed PHI in secure locations such as locked offices, cabinets or controlled workspaces; and

- d) Dispose of printed PHI by shredding or disposing of in locked shred bins in the workplace.

9. Electronic Records and System Access

When accessing electronic systems containing PHI, staff must:

- a) Only use their assigned login credentials;
- b) Access only the information necessary to perform assigned duties; and
- c) Log out or lock systems when work is complete.

10. Email and Electronic Communication

When sending PHI by email, staff must:

- a) Send PHI only to those who are authorized to receive the information based on their role within the HIPAA covered component, a HIPAA permitted purpose, or a valid release of information;
- b) Limit the amount of PHI to only the minimum necessary to accomplish the intended purpose;
- c) Verify recipient information prior to sending; and
- d) Encrypt emails when sending PHI outside of the agency.

This may be done by including the words “restricted information” in the e-mail subject line, or using Outlook email option “Encrypt.”

D. Separation of Covered Components

- 1. Because OYA operates as a hybrid covered entity, PHI related to TCM services must be protected from access by staff who are not part of the TCM healthcare component. (See section F, Uses and Disclosures of Protected Health Information, below for exceptions.)
- 2. OYA staff who are not assigned to TCM functions may only access TCM information when the information is necessary to perform their official job duties and is related to one of the following HIPAA permitted purposes:
 - a) Arranging, coordinating or continuing health care or health care related services for a youth, including connecting a youth with treatment, behavioral health services, or other services that support the youth’s health care needs;

- b) Providing continuity of care by ensuring necessary health or treatment information follows a youth between providers, placements, facilities, or other care settings; or
 - c) Protecting the health or safety of the youth, staff or others, safely transporting or transferring the youth, or maintaining the safety, security, and good order of a youth correctional facility.
- 3. A release of information (ROI) must be obtained before TCM PHI may be accessed by staff who have a business need that falls outside of the HIPAA permitted purposes above.
- 4. TCM notes in JJIS are automatically designated as protected information. When staff outside of the TCM healthcare component access a TCM note, they must document a business need related to one of the permitted purposes above. Access is logged within JJIS and regularly reviewed by the privacy officer.
- 5. External requests for TCM records must be handled through OYA's established records request process.
- 6. Questions about appropriate access, use or disclosure of TCM information must be referred to the privacy officer.

E. Privacy Incidents, Breaches and Complaints

- 1. Staff Reporting of Privacy or Security Incidents
 - a) Staff who believe PHI may have been accessed, used, or disclosed improperly must immediately report the incident to the privacy officer for investigation and to determine whether immediate mitigation steps are needed. Reports may be made verbally or in writing.
 - b) This is also considered an information security event. Staff must follow OYA policy I-D-3.3 Information Security Incident Response and immediately verbally report the event to their supervisor or the officer-of-the-day (OD), and the Information Services Service Desk (503) 378-4333. Voicemail is acceptable.

Staff must follow up the notification by reporting via email to ISWorkOrder@oya.oregon.gov, with "Information Security Event" as the subject.

2. Privacy Complaints from Youth

- a) Youth and their authorized personal representative have the right to file complaints regarding OYA's privacy practices or

compliance with HIPAA by submitting a privacy complaint to the designated privacy officer. Information for submitting complaints is included in the Notice of Privacy Practices, which is provided to all youth receiving TCM services and is available on OYA's website.

- b) Intimidation, coercion, discrimination or retaliation against youth who file a complaint or participate in an investigation is prohibited.
- c) Youth have the right to file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). Information on how to file an external complaint is included in the NPP YA 3060 form.
- d) Youth may also file a youth grievance in accordance with OYA policies II-F-1.1 Youth Grievance Process – Facility, or III-B-4.0 Youth Rights and Grievances in the Community. Staff responses to grievances may refer to paragraph c) above.

3. Review and Determination of Breach

All reported privacy or security incidents or complaints from staff or youth must be reviewed by the privacy officer to determine whether an impermissible use or disclosure of PHI has occurred and whether it constitutes a breach under HIPAA.

- a) After receiving report of an incident or a youth complaint, the privacy officer must:
 - (1) Record the date, time, and source of the report, a brief description of the incident, and any initial supporting documents (e.g., emails, screenshots);
 - (2) Review relevant information including case records, system activity, access logs, applicable policies, and HIPAA regulations;
 - (3) Consult with staff and youth, as needed; and
 - (4) Determine if immediate containment or mitigation is needed to prevent further unauthorized access, use or disclosure.
- b) The privacy officer must determine whether the incident constitutes a breach by assessing whether there has been an impermissible use or disclosure of PHI and if so, whether there is a low probability that the PHI has been compromised. The privacy officer must collaborate with

OYA's IS security officer (ISSO) when making this determination.

This determination will be based on HIPAA's required four factor risk assessment and will review:

- (1) The nature and extent of PHI involved;
 - (2) The unauthorized person who received or used the PHI;
 - (3) Whether the PHI was actually acquired or viewed; and
 - (4) The extent to which the risk has been mitigated.
- c) If a violation of privacy policies or HIPAA requirements is identified, the privacy officer must issue a corrective action plan.

4. Breach Notification

If it is determined that a breach occurred, the privacy officer must coordinate with Communications Office and OYA's IS security officer (ISSO) to initiate notification in accordance with 45 CFR § 164.400-414 and OYA policy I-E-3.3 Information Security Incident Response.

- a) OYA must notify impacted youth no later than 60 calendar days following discovery of the breach.
- b) If the breach affects fewer than 500 youth, OYA must report it to the Office of Civil Rights (OCR) no later than 60 days after the end of the calendar year in which the breach was discovered.
- c) If the breach affects more than 500 youth, OYA must report it to the OCR and notify prominent media outlets no later than 60 calendar days following discovery.
- d) If OYA does not have current contact information to provide written notice to the affected youth, substitute notice must be provided in accordance with HIPAA breach notification requirements.

5. Documentation and Retention

The privacy officer must document all reported incidents and privacy complaints throughout the investigation process, including intake details, investigation steps taken, risk assessment and

breach determination, findings and final disposition, corrective actions taken, and any required notifications.

All documentation must be retained for a minimum of six years.

F. Uses and Disclosures of Protected Health Information

1. OYA may use or disclose PHI without written authorization for activities related to treatment, payment, and healthcare operations (TPO) as defined in this policy.
2. OYA may use or disclose de-identified information in accordance with HIPAA requirements. De-identified information is health information that does not identify a youth and for which there is no reasonable basis to believe the information can be used to identify the youth.
3. OYA may also use or disclose PHI without authorization as permitted by HIPAA or as required by law. Examples include, but are not limited to:
 - a) Public health activities, such as reporting communicable disease or suspected child abuse or neglect;
 - b) Health oversight activities, such as providing information to state or federal agencies for audits, investigations or oversight;
 - c) Judicial and administrative proceedings, such as responding to a court order or subpoena or providing records for hearings;
 - d) Law enforcement purposes, such as providing information to locate or identify a youth; and
 - e) Disclosures to correctional institutions or law enforcement custodial settings, when necessary for the health, safety, security or administration of the youth or others.
4. Staff may access, use or share TCM PHI without an ROI when it is related to a HIPAA permitted purpose and is necessary to carry out their assigned job duties. When using or sharing information for a permitted purpose, staff must:
 - a) Access only the information necessary to accomplish the permitted purpose;
 - b) Use the information only for the purpose that justified the access; and

- c) Protect the confidentiality of the information by not using or disclosing it beyond what is needed to accomplish the permitted purpose.
- 5. When access to TCM PHI is required for a purpose that falls outside of the HIPAA permitted purpose identified in this policy, a valid ROI must be obtained before the information is accessed or disclosed.
- 6. External requests for TCM PHI must be referred to the OYA Records Office for review and response. This includes, but is not limited to:
 - a) Request for records or case files;
 - b) Requests for copies of documentation;
 - c) Subpoenas, court orders or other formal legal requests; and
 - d) Requests from external parties when the purpose or scope of the request is unclear.

G. Youth Rights Regarding Protected Health information

- 1. Youth have the right to access, review and request a copy of their protected health information, request corrections to information they believe is inaccurate or incomplete, and receive information about certain disclosures of their information.
- 2. Youth may submit these requests in writing directly to the privacy officer. Staff who receive a request for the type of information below must immediately forward it to the privacy officer for tracking and response.
- 3. Access to PHI

Youth have the right to inspect or obtain a copy of their PHI related to TCM services.

 - a) The agency must respond within 30 calendar days of receiving the request.
 - b) A one-time extension of up to 30 additional days is permitted if the youth is notified in writing of the delay and the reason.
 - c) Records must be provided in the format requested (electronic or paper), if readily available.
 - d) If the youth's request for access is denied, the agency must provide a written denial notice that includes the basis for denial, whether the denial is reviewable and instructions for submitting a complaint.

4. Youth have the right to request restrictions on the use of disclosure of their PHI.

OYA is not required to agree to requested restrictions. Requests may be denied if the restriction interferes with the agency's legal responsibilities, supervision of the youth, service delivery or safety and security operations.

5. Youth have the right to request to receive communications regarding their PHI by alternative means or at alternative locations.

OYA must consider reasonable requests; however, requests may be denied if they would interfere with the agency's operations, supervision responsibilities, or safety and security requirements.

6. Youth have the right to request an amendment to their protected health information if they believe the information is inaccurate or incomplete.

- a) The privacy officer must respond to amendment requests within 60 calendar days of receipt. A one-time extension of 30 additional days is permitted if the youth is provided a written explanation of the delay and the expected date of completion.
- b) If an amendment is approved, OYA must update the record and make reasonable efforts to inform those who may rely on the information.
- c) If an amendment request is denied, OYA must provide a written denial that includes the reason for denial, the youth's right to submit a statement of disagreement, and information on how to file a complaint. Any statement of disagreement submitted by the youth must be included with the record in future disclosures, as required by HIPAA.

V. OYA GENERAL OPERATING PROCEDURE REQUIRED: NO

VI. LOCAL OPERATING PROTOCOL REQUIRED: NO