# TABLE OF CONTENTS

# SECTION 16: REGULATORY COMPLIANCE

## FRAUD, WASTE and ABUSE (FWA)

Per State/Federal laws, APL 15-026, and DHCS contractual requirements, Health Plan is required to cooperate with the California Department of Health Care Services (DHCS) to identify Medi-Cal FWA cases including FWA prevention activities. FWA prevention is monitored and managed by the Health Plan's Compliance Department.

Health Plan performs audits to monitor compliance with standards, which could include, but are not limited to, billing requirements, adherence to appropriate coding guidelines, NCCI (Medicare National Correct Coding Initiative), and DHCS clinical policies. These audits can be used to identify the following examples of activities:

- Inappropriate "unbundling" of codes
- Claims for services not provided
- Up-Coding/Incorrect coding
- Potential overutilization
- Coding (diagnostic or procedural) not consistent with the Member's age/gender
- Improper use of benefits
- Use of exclusion codes
- High number of units billed
- Provider exclusion from Federally funded health care programs

As such, Health Plan is required to file a preliminary report with DHCS' Program Integrity Unit (PIU) detailing any suspected FWA cases identified by or reported to Health Plan on its network Providers within ten (10) working days of the discovery or notice of such FWA cases. Therefore, upon request, Providers are expected to cooperate, in a timely manner, with any FWA investigation activities which could include, but are not limited to, the following:

- Provide medical records.
- Provide additional electronic data.
- Provide other supporting documents as specified.
- Make all involved office staff or subcontracted personnel available for interviews, consultation, conferences, hearings, and in any other activities required in an investigation.
- Other requests associated with the FWA investigation

The Health Plan will refer subjects of FWA cases to state licensing boards through the California Department of Consumer Affairs when the evidence gathered warrants a referral.

To report suspected FWA cases, Providers can visit this anonymous reporting link. All reports made through this link can be anonymous. Providers can also email piu@hpsj.com to report suspected FWA cases. Provider training for FWA is covered in Training section.

## FALSE CLAIMS ACT

Per DHCS contractual requirements, Health Plan is required to provide its Network Providers with detailed information about the False Claims Act and other federal and State laws described in 42 USC section 1396a(a)(68), including information about the rights of employees to be protected as whistleblowers.

The False Claims Act is a federal law that makes it a crime for any person or organization to knowingly make a false record or file a false claim regarding any federal health care program, which includes any plan or program that provides health benefits, whether directly, through insurance or otherwise, which is funded directly, in whole or in part, by the United States Government or any state healthcare system.

"Knowingly" means:

- Actual knowledge of the information.
- Deliberate ignorance of the truth or falsity of the information.
- Reckless disregard of the truth or falsity of the information.
- Doesn't require proof of specific intent to defraud.

California False Claims Act (FCA) is more stringent than the Federal False Claims Act, because the FCA permits the Attorney General to bring a civil law enforcement action to recover treble damages and civil penalties against any person who knowingly makes or uses a false statement or document to either obtain money or property from the State or avoids paying or transmitting money or property to the State.

The California FCA also allows the "whistleblower" to receive a higher percentage of the recoveries and to participate even when prosecuted by the Department of Justice (DOJ) or Office of Attorney General (OAG).

Under the civil FCA, each instance of an item or a service billed to Medicare or Medi-Cal counts as a claim. California penalties start at $10,000 a claim.

There also is a criminal FCA. Criminal penalties for submitting false claims include imprisonment and criminal fines.

The federal False Claims Act protects employees who report a violation under the False Claims Act from discrimination, harassment, suspension, or termination of employment as a result of reporting possible fraud. Employees who report fraud and consequently suffer discrimination may be awarded:

- Two times their back pay plus interest.

- Reinstatement of their position without loss of seniority.
- Compensation for any costs or damage they incurred.

## HEALTH INFORMATION PRIVACY AND ACCOUNTABILITY ACT (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires Health Plan and all network Providers to protect the security and maintain the confidentiality of Member's Protected Health Information (PHI). PHI is any individually identifiable health information, including demographic information. PHI includes, but is not limited to, a Member's name, address, phone number, medical information, social security number, ID Card number, date of birth, and other types of personal information.

### Protecting PHI at Provider Sites

Providers are additionally required by 45 CFR parts 160 and 164 and DHCS Contract, Exhibit G to implement a comprehensive program to avoid unpermitted disclosure of PHI. Providers are required to implement a training program, and to have detailed office policies and procedures in place in order to comply with HIPAA requirements. These policies and procedures should include, but not be limited to:

- Keeping medical records secure and inaccessible to unauthorized access
- Limiting access to information to only authorized personnel, Health Plan, and any regulatory agencies
- Ensuring that confidential information is not left unattended in reception or patient care areas
- Safeguarding discussions in front of other patients or un-authorized personnel
- Providing secure storage for medical records
- Using encryption procedures when transmitting patient information
- Maintaining computer security
- Securing fax machines, printers, and copiers
- Published Privacy Practices

### Routine Consent

Member PHI can be appropriately disclosed for the following reasons (not an all-inclusive list):

- Verifying eligibility and enrollment
- Authorization for Covered Services
- Claims processing activities

- Member contact for appointments
- Investigating or prosecuting Medi-Cal cases (i.e., fraud)
- Monitoring Quality of Care
- Medical treatment
- Case Management/Disease Management
- Providing information to public health agencies permitted by law
- In response to court orders or other legal proceedings
- Appeals/Grievances
- Requests from State or federal agencies or accreditation agencies
- Providers must obtain specific written permission to use PHI for any reason other than the ones listed above.

### AB 1184 – Confidentiality of Medical Information

Providers are required to take specified steps to protect the confidentiality of a subscriber's or enrollee's medical information in regard to provided sensitive health care services:

- These rights are granted to protected individuals under Civil Code section 56.107.
- Communications need to be sent directly to the protected individual.
- A protected individuals request for communication to be sent to an alternative mailing address, email address, or telephone number should be honored.
- Medical information shouldn't be disclosed to anyone other than that individual (unless they have provided authorization).
- The form and format for confidential communications requested by a protected individual should be accommodated.
- All electronic communications should be directed to the protected individual.

### Member Access to Medical Records

Providers must ensure that their medical records systems allow for prompt retrieval of medical records and that these records are available for review whenever the Member seeks services. Member medical records should be maintained in a way that facilitates an accurate system for follow-up treatment and permits effective medical review or audit processes.

Medical records should be provided to Members upon reasonable request and should be organized, legible, signed, and dated.

### Psychotherapy Notes

Psychotherapy notes are an exception to the general rule of permitting the sharing of treatment information without the consent of the Member. Per 45 CFR §164.508(a)(2) psychotherapy notes are a special form of treatment information.

Per 45 CFR §164.508(b) and (c) authorization is a special and rigorous form of consent, which must include the following:

- A description of the information to be disclosed,
- The identity of the person or class of persons who may disclose the information
- To whom the information may be disclosed,
- A description of the purpose of the disclosure,
- An expiration date for the authorization,
- The signature of the person authorizing the disclosure.
- The individual signing the authorization can revoke it at any time
- The authorization for the release of psychotherapy notes must be a separate and independent document.

### HIPAA Minimum Necessary Rule [45CFR 164.502(b), 164.514(d)]

The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information (PHI). The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.

It is the Provider's responsibility to ensure that when sending documentation to Health Plan it is:

- Accurate
- For the correct Member
- Only includes documentation for the correct Member

### Reporting a Suspected of Confirmed Breach of PHI

A breach is an unauthorized disclosure of PHI that violates either Federal or State laws or PHI that is reasonably believed to have been acquired by an unauthorized person. This could include, but not be limited to:

- Release of Member's PHI to unauthorized persons.
- Misplacing or losing any electronic devices (e.g., thumb drive, laptop) that contain PHI.
- Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person.
- Any suspected privacy or security incident which risks unauthorized access to PHI and/or other confidential information.
- Any intrusion or unauthorized access, use or disclosure of PHI; or
- Potential loss of confidential information.

# SECTION 16: REGULATORY COMPLIANCE

## DHCS Reporting Obligations

If a Provider becomes aware of a suspected breach, the Provider must notify DHCS and HPSJ within 24 hours by email (or by telephone if unable to email DHCS and HPSJ) upon the discovery of the incident.

- The notice needs to be provided to the DHCS Program Contract Manager, the DHCS Privacy Office, and the DHCS Information Security Office, and the HPSJ Program Integrity Unit. Contact information is in the chart below.
- The notice needs to be made using the DHCS Privacy Incident Reporting Form and needs to include all information known at the time the incident is reported.
- Upon discovery of a breach or suspected security incident, intrusion, or unauthorized access, use, or disclosure of PHI, the Provider needs to take the following steps:
    - Immediately investigate such security incident or breach,
    - Take prompt action to mitigate any risks or damages involved with the security incident or breach, which should include attempting to retrieve the protected health information (PHI) if possible, and
    - Act as required by applicable Federal and State law.

Additionally, the Provider needs to provide a completed report of the investigation to the DHCS contacts and HPSJ within **ten (10) working days** of the discovery of the security incident or breach. This "Final PIR" must include the following:

- Any additional information not included in the Initial Form,
- Assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable federal and state laws,
- An action plan, and
- The implementation date of mitigation measures taken to halt and/or contain the improper use or disclosure.

If the Provider does not complete a Final PIR within the ten (10) working day timeframe, the Provider needs to request approval from DHCS within the ten (10) working day timeframe for a new submission timeframe.

If DHCS requests additional information, the Provider needs to make reasonable efforts to provide such information. A "Supplemental PIR" may be used to submit revised or additional information after the Final PIR is submitted. Any additional information submitted to DHCS, should also be sent to HPSJ.

## DHCS Determinations

DHCS will review the incident and determine if the incident was a breach. If the incident is determined to be a breach the following must be completed by the Provider:

- Notification to Affected Individuals: If the cause of a breach is attributable to a Provider

or its agents, the Provider needs to notify the affected individuals accordingly and shall pay all costs of such notifications, as well as all costs associated with the breach.
- The notifications need to comply with applicable federal and state law.
- DHCS needs to approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are sent out to HPSJ Members.

If the cause of a breach of PHI is attributable to a Provider or its agents, then the Provider is responsible for all required reporting of the breach as required by applicable federal and state law.

If Providers have any questions, they should email piu@hpsj.com.

DHCS and HPSJ Contact Information

| | |
|---|---|
| DHCS Program Contract Manager | Travis Romo<br>Travis.Romo@dhcs.ca.gov |
| DHCS Privacy Office | Privacy Office<br>C/O: Office of HIPAA Compliance<br>Department of Health Care Services<br>P.O. Box 997413, MS 4722<br>Sacramento, CA 95899-7413<br>Email: incidents@dhcs.ca.gov<br>Telephone: (916) 445-4646 |
| DHCS Information Security Office | Information Security Office<br>DHCS Information Security Office<br>P.O. Box 997413, MS 6400<br>Sacramento, CA 95899-7413<br>Email: incidents@dhcs.ca.gov |
| HPSJ Program Integrity Unit | Compliance Analyst: Raji Bahia<br>Email: piu@hpsj.com<br>Telephone: (209) 425-4354 |

## TRAINING

Federal and state laws require new Providers and their employees complete HIPAA, FWA, and Diversity, Equity and Inclusion (DEI) trainings within 30 days of being placed on active status, annually thereafter, and for new employees within 30 days of hire. Providers will need to furnish documentation to Health Plan as proof the trainings were completed at the required intervals, annually, and within 30 days of hire for new employees. Provider Services will send out a curtesy reminder when annual trainings are due. It is the duty of the Provider to submit proof to Health Plan that training was completed within 30 days of hire for new employees. This should be submitted to Health Plan upon completion through the year for new hires.

Providers must furnish to Health Plan the following: training source, training date, list of other Providers in practice with NPIs and employees trained, and attestation of completion. The source of the training can be one of three options; stream Health Plan trainings from our website, download a pdf of the trainings from our website, or use other training. If the training source is other, an outline of the content, or a copy of the training, or a URL link to the training source must be provided.

Health Plan has three online Attestation links, one for each training, where Providers can attest to training completion for all Providers and employees in your practice and enter/upload all of the information specified in the previous paragraph. The attestation links can be found here Provider Trainings - Health Plan of San Joaquin (hpsj.com).