TABLE OF CONTENTS

SECTION 16: REGULATORY COMPLIANCE

FRAUD, WASTE and ABUSE (FWA)

Per State/Federal laws, APL 15-026, and DHCS contractual requirements, HPSJ 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 HPSJ Compliance Department.

HPSJ 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, HPSJ is required to file a preliminary report with DHCS' Program Integrity Unit (PIU) detailing any suspected FWA cases identified by or reported to HPSJ 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

HPSJ 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.

HEALTH INFORMATION PRIVACY AND ACCOUNTABILITY ACT (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that requires HPSJ 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, HPSJ, 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 HPSJ it is:

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

Reporting a Breach of PHI

A breach is an unauthorized disclosure of Protected Health Information (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

If a Provider becomes aware of a **suspected breach**, the Provider must report the

breach within 24 hours of discovery) to DHCS by submitting privacy incident through DHCS's portal DHCS Privacy Incident Report Internet Process. Providers are also required to notify the HPSJ Program Integrity Unit inbox at piu@hpsj.com within the same time frame. If the provider is unable to email immediately upon discovery, the Provider shall provide notice by telephone to DHCS at (866) 866-0602 and to HPSJ at (855) 400-6002.

The Provider must also submit the DHCS required updates for each incident at 72 hours and 10 days after the suspected breach through the same DHCS portal stated in the previous paragraph and also notify the HPSJ Program Integrity Unit inbox at piu@hpsj.com when these updates are submitted. Providers are expected to keep both DHCS and HPSJ informed timely, via email or conference calls, until the incident is remediated and resolved after the 10-day requirements. Providers are also expected to provide documentations to show evidence of compliance upon requests by DHCS and/or HPSJ.

If Providers have any questions, they should email piu@hpsj.com. The Provider will also be responsible for investigating mitigating, and implementing a corrective action plan to prevent the incident from reoccurring. Report suspected breaches anonymously through this link.

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 HPSJ 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 to HPSJ proof training was completed within 30 days of hire for new employees. This should be submitted to HPSJ upon completion through the year for new hires.

Providers must furnish to HPSJ 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 HPSJ 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.

HPSJ 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).

SECTION 16: REGULATORY COMPLIANCE