TABLE OF CONTENTS

SECTION 16: REGULATORY COMPLIANCE

FRAUD, WASTE, AND ABUSE (FWA)

Per State/Federal laws, APL 15-026, 42 CFR § 455.12 – 455.23, 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 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 (CMS National Correct Coding Initiative), and DHCS clinical policies. These audits can be used to identify the following examples of activities:

- Inappropriate "unbundling" of codes
- Inappropriate use of modifiers
- 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.

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 the 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 INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA), CONFIDENTIALITY MEDICAL INFORMATION ACT (CMIA) & CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (CCPA)

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), whereas the Confidentiality Medical Information Act (CMIA) is a California state law that offers extra safeguards for member's 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. Additionally, Health Plan considers member Personal Information (PI), such as, race/ethnicity, language, gender identity, and sexual orientation the same as PHI and applies the same safeguards.

In addition to Health Insurance Portability and Accountability Act (HIPAA) 45 CFR Parts 160 and 164, Health Plan's contracted Third Parties are also required to abide by the applicable laws and regulations imposed on Health Plan by both state and federal government agencies listed below:

1. Health Information Technology for Economic and Clinical Health Act (HITECH Act).
2. Confidentiality of Medical Information Act (CMIA) section 56 et al.
3. Department of Health Care Services (DHCS) Contract as amended.
4. The Knox-Keene Health Care Service Plan Act of 1975, as amended.
5. California Consumer Privacy Act of 2018 Section 1798.100.
6. Information Practices Act (IPA) at California Civil Code section 1798.3(a)
7. The Privacy Act 5 U.S.C. 552a, as amended.
8. "Exhibit G Business Associate Addendum" ("Exhibit G") of the DHCS Contract.

When this Manual refers to "PHI/PI", it is collectively referring to PHI and PI including race/ethnicity, language, gender identity, and sexual orientation.

Protecting PHI/PI 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/PI. 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 are not 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/PI 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/PI for any reason other than the ones listed above.

REQUIREMENTS APPLICABLE TO SENSITIVE SERVICES

Sensitive Services are defined by AB 1184 and include services described in sections 6924-6930 of the Family Code and sections 121020 and 124260 of the California Health and Safety Code. Below are the areas of health services that qualify as sensitive services:

- Mental or behavioral health
- Drug and alcohol abuse
- Communicable diseases
- Sexual and reproductive health
- Sexually transmitted infections
- Substance use disorders

- Gender-affirming care
- Intimate partner violence

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 regarding 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 individual's 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.

AB 254 - Confidentiality of Medical Information Act Regarding Reproductive or Sexual Health Application Information

AB 254 revises the definition of medical information to include reproductive or sexual health application information. If a health care Provider offers a reproductive or sexual health digital service to a consumer for a purpose of allowing that individual to manage their information or for the diagnosis, treatment, or management of a medical condition, then that health care Provider will be subject to the requirements of the Confidentiality of Medical Information Act.

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.

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.

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

- Release of a Member's PHI/PI to unauthorized persons.
- Misplacing or losing any electronic devices (e.g., thumb drive, or laptop) that contains PHI/PI.
- Unsecured PHI/PI, if the PHI/PI 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/PI and/or other confidential information.
- Any intrusion or unauthorized access, use or disclosure of PHI/PI; or
- Potential loss of confidential information.

Provider Reporting Obligations, for Medi-Cal Enrolled Providers

If a Medi-Cal enrolled Provider becomes aware of a suspected breach, the Provider must notify DHCS within 24 hours of discovery of the incident/breach. Additionally, Health Plan requests Providers to notify Health Plan's PIU upon the discovery of the incident/breach by emailing or calling the Privacy Officer at the following email or phone number.

Privacy Officer
Email: piu@hpsj.com
Telephone: 1-209-933-3611

If the provider isn't Medi-Cal enrolled, then the notice will be provided to DHCS by Health Plan on behalf of the provider. Refer to the next section for more direction on this scenario.

How to Submit a Breach/Incident to DHCS
If the Provider is Medi-Cal enrolled, the Provider should submit the notification through the DHCS Privacy Reporting Portal within 24 hours of discovering the incident. If the DHCS Privacy Reporting Portal isn't available then Health Plan/Provider will fill out this privacy incident form and email it to incidents@dhcs.ca.gov with a copy to the DHCS Program Contract Manager, and the DHCS Information Security Office.

The Provider should complete the following actions upon discovery of a suspected or confirmed incident/breach, security breach, intrusion, unauthorized access, use, or disclosure of PHI:

1. Immediately investigate such security incident or breach.
2. Take prompt action to mitigate any risks or damages involved with the security incident or breach, which should include attempting to retrieve the PHI/PI if possible.
3. Act as required by applicable Federal and State law.

In addition to the 24-hour required reporting of the incident/breach, the Provider needs to provide three (3) updates to DHCS on the incident/breach; update, 1.) a 72-hour update of the investigation, and 2.) Final Report of the investigation to DHCS within ten (10) working days of the discovery of the suspected security incident or breach. This Final Report must include the following:

1. An assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable Federal and State laws.
2. Detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure.
3. If DHCS or Health Plan requests additional information the Provider will make reasonable efforts to provide Health Plan with such information. Health Plan will provide the additional requested information to DHCS on the Provider's behalf.

If the Provider needs more than ten (10) working days to conduct and complete the Final Report, the Provider must notify the DHCS to request approval for a new submission timeframe for the Final Report. The Provider acknowledges that a new submission timeframe requires the approval of the DHCS.

If the mitigation and corrective action plan steps haven't been implemented and completed by the 10-day time period, then the Provider will continue to provide Health Plan with a weekly update until all mitigation and corrective action plan steps for the security incident or breach have been completed.

Provider Reporting Obligations for Providers, that are Not Medi-Cal Enrolled

If a non-Medi-Cal enrolled Provider becomes aware of a suspected breach, the Provider must notify Health Plan within 24 hours of discovery of the incident/breach. Notify Health Plan's PIU upon the discovery of the incident/breach by emailing or calling the Privacy Officer at the following email or phone number.

Privacy Officer
Email: piu@hpsj.com
Telephone: 1-209-933-3611

Actions Health Plan Will Take on Behalf of the Provider and Provider's Obligations to Supply Information to Health Plan

The Provider should complete the following actions upon discovery of a suspected or confirmed incident/breach, security breach, intrusion, unauthorized access, use, or disclosure of PHI/PI:

1. Immediately investigate such security incident or breach.
2. Take prompt action to mitigate any risks or damages involved with the security incident or breach, which should include attempting to retrieve the PHI/PI if possible.
3. Act as required by applicable Federal and State law.

In additional to the 24-hour required reporting of the incident/breach, the Provider will need to provide three (3) updates to Health Plan, so Health Plan can report to DHCS at the following intervals on be-half of the Provider; 1.) a 72-hour update of the investigation, and 2.) Final Report of the investigation to DHCS within ten (10) working days of the discovery of the suspected security incident or breach. This Final Report must include the following:

1. An assessment of all known factors relevant to a determination of whether a breach occurred under HIPAA and other applicable Federal and State laws.
2. Detailed corrective action plan, including its implementation date and information on mitigation measures taken to halt and/or contain the improper use or disclosure.
3. If DHCS or Health Plan requests additional information the Provider will make reasonable efforts to provide Health Plan with such information. Health Plan will provide the additional requested information to DHCS on the Provider's behalf.

If the Provider needs more than ten (10) working days to conduct and complete the Final Report, the Provider must notify Health Plan so Health Plan can request approval on behalf of the Provider for a new submission timeframe for the Final Report. The Provider acknowledges that a new

submission timeframe requires the approval of the DHCS. Health Plan will communicate to the Provider DHCS's decision if an extension will be granted.

If the mitigation and corrective action plan steps haven't been implemented and completed by the 10-day time period, then the Provider will continue to provide Health Plan with a weekly update until all mitigation and corrective action plan steps for the security incident or breach have been completed.

Determinations

- DHCS will review the details in the Final Report and determine if the suspected or confirmed incident/breach, security breach, intrusion, unauthorized access, use, or disclosure of PHI/PI is a breach. If DHCS determines the suspected or confirmed incident/breach, security breach, intrusion, unauthorized access, use, or disclosure of PHI is a breach then individual member breach notifications are required. If the cause of a breach of PHI/PI is attributable to the Provider or its subcontractors, the Provider agrees that Health Plan shall make all required reporting of the breach as required by applicable Federal and State law, including any required notifications to media outlets, the Secretary, and other government agencies/regulators.
- DHCS will approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made.
- The notifications will comply with applicable Federal and State law.

Additionally, Health Plan will review and approve or reject the Providers corrective action plan. If the CAP is rejected by Health Plan, Health Plan will work with the Provider on the CAP.

Law Enforcement Hold on Notification of Breach

If the Provider has received notification from law enforcement that requires a delay, the Provider will delay notification to individuals of the security incident, breach, or unauthorized use or disclosure of PHI or confidential data. This direction will occur if or when such notification would impede a criminal investigation or damage national security and whether such notice is in writing, and whether Section 13402 of the HITECH Act (codified at 42 U.S.C. § 17932), California Civil Code §§ 1798.29 or 1798.82, or any other federal or state laws requiring individual notifications of breaches are triggered. If a delay is requested of the Provider, the Provider will notify Health Plan. Health Plan is fully committed to cooperating with directives from stated law enforcement agencies. This includes enforcing compliance from Providers and ensuring their cooperation with investigations and prosecutions.

DHCS and Health Plan agree to not request the Provider to use or disclose PHI/PI in any manner that would not be permissible under HIPAA and/or other applicable Federal and/or State law.

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

SECTION 16: REGULATORY COMPLIANCE

TRAINING

Federal and state laws require new Providers and their employees to complete HIPAA, FWA, Diversity, Equity, and Inclusion (DEI), Transgender, Gender Diverse, Intersex (TGI), and Non-specialty Mental Health Services (NSMHS) 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 courtesy 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
- Employees trained
- 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 their practice and enter/upload all the information specified in the previous paragraph. The attestation links can be found here Provider Trainings (hpsj.com).