
SECTION 16: REGULATORY COMPLIANCE

Section 16: Regulatory Compliance	16-1
Fraud, Waste, and Abuse	16-1
Health Information Privacy and Accountability Act (HIPAA)	16-1
Training	16-3

SECTION 16: REGULATORY COMPLIANCE

FRAUD, WASTE, AND ABUSE

HPSJ cooperates with the California Department of Health Care Services (DHCS) in working to identify Medi-Cal fraud, waste, and abuse. Fraud and abuse prevention is monitored and managed by the HPSJ Compliance Department.

HPSJ performs audits to monitor compliance with standard billing requirements. These audits can be used to identify the following activity (not an all-inclusive list):

- 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

When required, HPSJ will report suspected fraud and/or abuse to the DHCS and Department of Justice (DOJ) Bureau of Medi-Cal Fraud. Providers must cooperate in potential investigations by making office staff and subcontracted personnel available for interviews, consultation, conferences, hearings, and in any other activities required in an investigation.

To report potential occurrences of fraud, waste, and abuse Providers can visit <https://www.lighthouse-services.com/StandardCustomURL/LHILandingPage.asp>

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.

HPSJ Efforts to Protect PHI

HPSJ has a comprehensive training program as well as detailed policies governing the protection of PHI. In addition, all HPSJ staff with access to PHI are trained on privacy and information

SECTION 16: REGULATORY COMPLIANCE

security laws to ensure full compliance. Member information on HPSJ computers can only be accessed by authorized staff and all computer servers are protected from theft and natural disasters.

HPSJ also makes sure that Members are notified of the plan's privacy practices, advised of their privacy rights, and informed as to how to obtain written information or file a complaint regarding a potential violation of their privacy rights.

Protecting PHI at Provider Sites

Providers are required to have 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

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

SECTION 16: REGULATORY COMPLIANCE

- 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.

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.

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

If a Provider becomes aware of a breach, the Provider must notify HPSJ immediately (within 24 hours of becoming aware) by contacting the HPSJ Provider Services Department at (209) 942-6340 or submit a report online:

https://www.lighthouse-services.com/_StandardCustomURL/LHILandingPage.asp

TRAINING

Federal law requires new providers and employees to complete the HIPAA and FWA and abuse training within 30 days of being placed on active status, and annually thereafter.

HPSJ provides training and education for all network providers and their staff related to FWA and HIPAA annually. A signed attestation of the completion of training is required for all network providers and their staff. FWA and HIPAA training and attestation can be found on HPSJ's provider portal.