1. **Policy Statement**

Santa Clara Family Health Plan (the Plan) will not use or disclose protected health information, except either: (1) as the Privacy Rule and applicable state law and government contracts permit or require; or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing.

2. **Purpose**

The purpose of this policy is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed by the Plan, its providers, staff and/or Business Associates.

3. **Definitions**

See HIPAA Privacy Rule – Definitions Policy and Procedure Number LC-11-01.

4. **Procedures**

This policy applies to the Plan and its providers (both of which are “covered entities”) and also to their respective staffs and Business Associates (all of whom are hereinafter referred to as “Staff”).

Authority: 45 CFR §§164.502, 164.506, 164.508, 164.510, and 164.512
A. **General Rule:** The staff may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing. However, the staff must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. (Please see Policy CP016 for more information about the Minimum Necessary Rule.)

B. **Request for Disclosure:** If staff receives a request to disclose protected health information, the employee may disclose the requested information if:
   1. He/she has confirmed that disclosure is required or permitted under HIPAA, and
   2. It has been confirmed that the member has not placed a restriction on the disclosure of his or her PHI.

C. **Privacy Official Verification**
   If staff or a business associate is at all unsure whether use or disclosure is permitted or required without member authorization, the employee must request an opinion of the Privacy Official. To obtain Privacy Official verification, the employee must complete the Privacy Issue Request Form, (available on SCFHP’s Intranet). If the information is needed on an expedited basis, and the Privacy Official cannot be reached, the employee may consult with his or her Department Supervisor. With the Department Supervisor’s verification that the use or disclosure is permitted or required under HIPAA and that the individual has not restricted disclosure, the Privacy Official may be notified after the disclosure.

D. **Required Disclosures.** The staff is required to disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action. However, before making any such disclosure, the staff should discuss the disclosure with the Privacy Officer. Requests for disclosure to HHS should be referred by Plan staff to the Compliance Department for response.

E. **Uses and Disclosures that Do Not Require Authorization.** The staff is permitted, but not required, to use and disclose protected health
information, without an individual’s authorization, for the following purposes or situations. If the request for disclosure is for routine, recurring disclosures, or is a request that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the permissible disclosure, the Plan staff may respond to the requestor. The following uses and disclosure of protected health information do not require authorization from the individual.

1. **Treatment, Payment, Health Care Operations.** The staff may use and disclose protected health information for its own treatment, payment, and health care operations activities. The staff also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. The terms “Treatment”, “Payment” and “Health Care Operations” are defined in Policy # CP008. But staff should keep in mind that the terms are broadly used:

   a. **Treatment.** Staff may use and disclose an individual’s PHI without authorization to:

      i. provide, coordinate, or manage the health care and related services by one or more health care providers, including the coordination or management of health care;
      ii. consult with health care providers, or
      iii. refer a patient from one health care provider to another;

   b. **Payment.** Staff may use and disclose an individual’s PHI without authorization to:

      i. obtain or provide reimbursement for health care services,
      ii. set and collect premiums
      iii. determine which benefits will be reimbursed or paid for
iv. determine who has financial responsibility for health care services
v. determine if an Individual is eligible for care and the extent of coverage (e.g., coordination of benefits, subrogation, whether copayments or other insurance apply)
vi. adjudicate claims, bill and collect amounts due; obtain payment under reinsurance
vii. underwriting
viii. review health care services with respect to medical necessity, coverage, appropriateness or justification of charges
ix. utilization review, and
x. report individuals to consumer reporting agencies following collection actions.

c. Health care operations. Staff may use and disclose an individual’s PHI without authorization to conduct:

i. quality assessment and improvement activities;
ii. peer review, credentialing or other and similar performance evaluations;
iii. underwriting, premium rate setting, reinsurance and other risk related tasks;
iv. conducting or arranging for medical review;
v. legal services, and auditing functions, including fraud and abuse detection and compliance programs;
vi. member service functions and resolution of member grievances;
vii. business management, planning and development, including practice management and support; and
viii. general administrative activities of the Covered Entity

An exception to the general “treatment” rule applies to psychotherapy notes. Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.

Even if authorization is not required for payment treatment and health care operations, obtaining permission from individuals to use
and disclose their protected health information is always permissible.

If the Staff has any questions about whether a use or disclosure without authorization is permissible, please discuss the matter with the Privacy Officer of the Plan or, if applicable, of the provider.

4. **Public Interest and Benefit Activities.** Staff or business associates may use and disclosure of protected health information, without an individual’s authorization or permission, for the 12 “national priority purposes” described below. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, in an effort to balance the individual privacy interest and the public interest need for this information. If the request is for routine, recurring disclosures, or requests for disclosures that limit the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure, the Staff may respond directly to the requestor. However, for any other request for disclosure, the Plan Staff must contact the Privacy Officer for advice before using or disclosing protected health information for these “national priority purposes”, so the Privacy Officer can determine: whether the Plan should comply with or refuse the requested use or disclosure and, if the Plan will comply with the request, which Plan department will make the disclosure. With the approval of the Privacy Officer, the following uses and disclosures are permissible without authorization:

a. **Required by Law.** The Staff may use and disclose protected health information without individual authorization as required by law (including by statute, regulation, or court orders).

b. **Public Health Activities.** The Staff may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product
recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.

c. **Victims of Abuse, Neglect or Domestic Violence.** In certain circumstances, the Staff may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

d. **Health Oversight Activities.** The Staff may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as DMHC, DHCS or CMS audits or investigations necessary for oversight of the health care system and government benefit programs.

e. **Judicial and Administrative Proceedings.** The Privacy Rule permits the Staff to disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided. All subpoenas received by Plan Staff must be forwarded to the Executive Assistant to the CEO or to the Compliance Department so that they can verify that the subpoena is valid and not overreaching, confirm that the individual has not filed an objection to the subpoena, and obtain authorization of the individual if they feel it is advisable to protect the Plan from liability.

f. **Law Enforcement Purposes.** The Staff may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas)
and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official’s request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person’s death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

g. **Decedents.** The Staff may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

h. **Cadaveric Organ, Eye, or Tissue Donation.** The Staff may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

i. **Research.** All requests for use or disclosure of protected health information for research purposes must be discussed with the Privacy Officer because of the many conditions and limitations placed on the use for this purpose by the Privacy Rule. Those conditions and limitations include the following: The Privacy Rule permits the Staff to use and disclose protected health information for research purposes, without an individual’s authorization, provided the Staff obtains either: (1) documentation that an alteration or waiver of individuals’ authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the
use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought. The Staff also may use or disclose, without an individuals’ authorization, a limited data set of protected health information for research purposes (see discussion below).

j. **Serious Threat to Health or Safety.** The Staff may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). The Staff may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

k. **Essential Government Functions.** An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: intelligence and national security activities that are authorized by law, providing protective services to the President, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.

l. **Workers’ Compensation.** The Staff may disclose protected health information as authorized by, and to comply with, workers’ compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

3. **Incidental Use and Disclosure.** The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as “incident to,” an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the “minimum necessary,” as required by the Privacy Rule. For example, the Plan or a provider may maintain a sign in sheet at the front desk. The fact that persons who sign in later may see that a member is visiting
the Plan is an incidental use or disclosure and is not a violation of that member’s privacy.

4. **Uses and Disclosures that Require the Individual to have an Opportunity to Agree or Object.** For the following uses and disclosures of PHI, the Staff must obtain informal permission by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, Staff generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual. The Staff must document in the Member Services Database and the Privacy Officer Database – or the provider’s equivalent data bases - any informal conversation with a member in which the member gives or withhold consent to the use and disclosure of PHI.

   a. **Facility Directories.** It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A health care provider may rely on an individual’s informal permission to list in its facility directory the individual’s name, general condition, religious affiliation, and location in the provider’s facility. The provider may then disclose the individual’s condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

   b. **For Notification and Other Purposes.** The Staff also may rely on an individual’s informal permission to disclose to the individual’s family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person’s involvement in the individual’s care or payment for care. This provision, for example, would allow a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, the Staff may rely on an individual’s informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual’s care of the individual’s location, general condition, or death. In addition, protected
health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts. But the Staff must be careful to make certain that only protected health information that is directly relevant to the person’s involvement in the individual’s care is used or disclosed without more formal authorization.

6. **Limited Data Set.** A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set. The identifiers that have to be removed for protected health information to be considered a limited data set include:

   a. Names;
   b. Postal address information, other than town or city, State, and zip code;
   c. Telephone numbers;
   d. Fax numbers;
   e. Electronic mail addresses;
   f. Social security numbers;
   g. Medical record numbers;
   h. Health plan beneficiary numbers;
   i. Account numbers;
   j. Certificate/license numbers;
   k. Vehicle identifiers and serial numbers, including license plate numbers;
   l. Device identifiers and serial numbers;
   m. Web Universal Resource Locators (URLs);
   n. Internet Protocol (IP) address numbers;
   o. Biometric identifiers, including finger and voice prints; and
   p. Full face photographic images and any comparable images.

F. **Uses and Disclosures that Require the Individual’s Authorization**

1. **General Rule:** The Staff must obtain the individual’s written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care
operations or otherwise permitted or required by the Privacy Rule. The Staff may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. To determine what those circumstances are, please contact the Privacy Officer.

2. **In Writing.** An authorization must be written and contain specific terms described in Policy CP015. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual’s authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

3. **Plain Language.** All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data described in Policy CP015.

4. **Psychotherapy Notes.** A covered entity must obtain an individual’s authorization to use or disclose psychotherapy notes with the following exceptions:
   
   - The covered entity who originated the notes may use them for treatment.
   - A covered entity may use or disclose, without an individual’s authorization, the psychotherapy notes for its own training and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity’s compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as otherwise required by law.

5. **Marketing.** The Staff must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual, and for a covered entity’s provision of promotional gifts of nominal value. An authorization for marketing that involves the covered entity’s receipt of direct or indirect payment from a third
party must reveal that fact. No authorization is needed, however, to
make a communication that falls within one of the exceptions to the
marketing definition. See Policy CP008 for the definition of
marketing and the list of excepted activities that will not be
considered marketing.

G. **Accounting.** Individuals have a right to an accounting of the disclosures of their
protected health information by a covered entity or the covered entity’s business
associates. As the Staff discloses protected health information pursuant to this
policy, the Staff must report the disclosure to the Plan or Provider Privacy Officer
for recording in the accounting data base. Please see Policy CP013 for more
information about the Accounting requirements of the Privacy Rule and how to
comply.

5. **Confidentiality of Information**

In accordance with SCFHP’s Confidentiality Policy, and all applicable state and
federal laws, any and all information that is required to be kept confidential, shall
be kept confidential.

6. **Recordkeeping**

Each department is responsible for retaining and maintaining
documents/records/paperwork for a minimum of ten (10) years for their
own department (refer to policy LC-07-04 Record Retention).