Notice of Privacy Practices

Effective: January 1, 2024

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

In this notice we use the terms “we,” “us,” and “our” to describe Santa Clara Family Health Plan (SCFHP).

SCFHP is required by state and federal law to protect your health information. We also require all contracting providers and vendors to protect your health information. We must give you this notice that tells how we may use and share your information. It also tells you what your rights are.

Your Information is Personal and Private

We get information about you from you, Federal, State, and local agencies while you apply and after you are eligible to enroll in our health plan. We also get medical information from your health care providers, clinics, labs, and hospitals so we can approve and pay for your health care services received.

What is “Protected Health Information”?

Your protected health information (“PHI”) is health information that contains identifiers, such as your name, Social Security number, or other information that reveals who you are. For example, your medical record is PHI because it includes your name and other identifying information.

Our staff follows policies and procedures that protect your health information given to us in oral, written or electronic methods. Our staff goes through training that covers the internal methods members’ oral, written and electronic PHI may be used or disclosed across the organization. All our staff with access to your health information is trained on our privacy policy and information security laws. Our staff has access only to the minimal amount of information they need to do their job.

Our employees also follow internal practices, policies and procedures to protect any conversations about your health information. For example, employees are not allowed to speak about your information in the elevator or hallways. Employees must also protect any written or electronic documents containing your health information across the organization.

Our computer systems protect your electronic PHI at all times by using various levels of password protection and software technology. Fax machines, printers, copiers, computer screens, workstations, and portable media disks containing your information are carefully guarded from others who should not have access. Employees must ensure member PHI is picked up from fax machines, printers and copiers and only is received by those who have access. Portable media devices with PHI are encrypted and must have password protections applied. Computer screens must be locked when employees are away from their desks and offices. Workstation drawers and cabinets that contain PHI have secure locks placed on them.

We will also protect, access, and use race/ethnicity, language, gender identity, and sexual orientation data in the same way we do for PHI. We will not use race/ethnicity, language, gender identity, and sexual orientation data for setting rates or to deny services, coverage, and benefits.

Changes to Notice of Privacy Practices

We must uphold the notice that we are using now. We have the right to change these privacy practices. Any changes in our practices will apply to all of your medical information. If we do make changes required by law, we will notify you.

How We May Use and Share Information about You

Your information may be used or shared by us only for treatment, payment and health care operations. Some of the information we use and share is:

- Your name,
- Address,
- Personal facts,
- Medical care given to you,
- The cost of your medical care, and
- Your medical history.

Some actions we take when we act as your health plan include:

- Checking whether you are covered,
- Approving, providing, and paying for services,
- Investigating or prosecuting cases (like fraud),
- Checking the quality of care you receive,
- Making sure you get all the care you need.

Some examples of why we would share your information with others involved in your health care are:

- **For treatment**: You may need medical treatment that needs to be approved ahead of time. We will share information with health care providers, hospitals, and others in order to get you the care you need.
- **For payment**: We use your PHI to pay for health care claims sent to us for your medical care. When we do this, we share information with the health care providers, clinics, and others who bill us for your care. And we may forward bills to other health plans or organizations for payment.
- **For health care operations**: We may use information in your health record to check the quality of the health care you receive. We may also use this information in audits, programs to stop fraud and abuse, planning and general administration.
- **For business associates**: We may use or disclose your PHI to an outside company that assists us in operating our health system.

Other Uses for your Health Information

The following is a description of other possible ways in which we might (and are permitted to) use and/or disclose your protected health information:

- We may give out medical information to a health oversight agency for activities authorized by law. These oversight activities may include audits, investigations, inspections and licensure or disciplinary actions. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.
- You or your physician, hospital, and other health care providers may not agree if we decide not to pay for your care. We may use your health information to review these decisions.
- We may share your health information with groups that check how our health plan is providing services.
- We may share information with persons involved in your health care, or with your personal representative.
- We must share your health information with the federal government when it is checking on how we are meeting privacy rules.
- We may share your health information with organizations that obtain, bank or transplant organs or tissue donations.
- We may share your health information about a worker’s compensation illness or injury following written request by your employer, worker’s compensation insurer, or their representatives.

- We may use and share your health information for certain kinds of research.
- We may use and share your information to assess health disparities and improve patient-centered care as part of our health equity effort. Your preferred spoken and written languages are shared with provider groups.
- We may give out your information for public health activities. These activities may include, but are not limited to the following:
  - » To prevent or control disease, injury, or disability;
  - » To report births and deaths;
  - » To report child abuse or neglect;
  - » To report problems with medications and other medical products;
  - » To notify people of recalls of products they may be using; and
  - » To notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.

When Written Permission is Needed

If we want to use your information for any purposes not listed above, we must get your written permission. If you give us your permission, you may take it back in writing at any time.

What Are Your Privacy Rights?

You have the right to ask us not to use or share your protected health care information. We are not required to agree and may not agree if it will affect your health care needs.

You have the right to ask us to contact you only in writing or at a different address, post office box, or by telephone. We will accept reasonable requests when we can readily produce the information in the way you specified.

You and your personal representative have the right to get a copy of your health information. You will be sent a form to fill out to tell us what you want copied. You may have to pay for costs of copying and mailing records. We may keep you from seeing certain parts of your records for reasons allowed by law.

You have the right to ask that information in your records be changed if it is not correct or complete. You will be sent a form to fill out to tell us what changes you want. We may not agree to your request if:

- The information is not created or kept by SCFHP, or
- The information is not part of a standard set of information kept by SCFHP, or
- The information has been gathered for a court case or other legal actions, or

- We believe it is correct and complete.

We will let you know if we agree to make the changes you want. If we don't agree to make the changes you want, we will send you a letter telling you why. You may ask that we review our decision if you disagree with it. You may also send a statement saying why you disagree with our records. We will keep your statement with your records.

Important: Santa Clara Family Health Plan does not have complete copies of your medical records. If you want to look at, get a copy of, or change your medical records, please contact your physician or clinic.

When we share your health information you have the right to request a list of:

- Whom we shared the information with,
- When we shared it,
- For what reasons, and
- What information was shared.

This list will not include when we share information with you, with your permission, or for treatment, payment, or health plan operations.

You have a right to request a printed paper copy of this Notice of Privacy Practices.

You can also find this notice on our website at **www.scfhp.com**.

Privacy Breach

Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of a member's personal information maintained by SCFHP. Good faith acquisition of a member's personal information by an employee or agent of SCFHP for the purposes of SCFHP is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

Personal information means a member's first name or first initial, and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: 1) Social Security number; 2) driver's license number or California identification card number; 3) credit or debit card number, or account number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; 4) medical information; or 5) health insurance information. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Medical information means any information regarding a member's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. Health insurance information

means a member's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the member, or any information in a member's application and claims history, including any appeals records.

In the event that an unauthorized person acquires private health information of SCFHP's members, SCFHP will disclose the breach to the affected members as quickly as possible, without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The security breach notification to members shall be written in plain language, and include (at a minimum), the name and contact information of the member who is reasonably believed to have been the subject of the breach. If any of the following information is possible to determine at the time the notice is provided, then the notification shall include: the date of the breach; or the estimated date of the breach; or the date range within which the breach occurred. The notification shall also include: the date of the notice; whether the notification was delayed as a result of law enforcement investigation; a general description of the breach incident; and the toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a Social Security number, a driver's license number, or a California identification card number. At the discretion of SCFHP, the notification may also include: information about what SCFHP has done to protect members whose information has been breached; and/or advice on steps that the member whose information has been breached may take to protect him/herself.

The security breach notification may be provided by one of the following methods: 1) written notice; 2) electronic notice; or 3) substitute notice. A substitute notice may be used if SCFHP demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or the number of affected members to be notified exceeds 500,000, or when SCFHP does not have sufficient contact information. Substitute notice shall consist of all of the following: 1) email notice when SCFHP has an email address for the affected member; 2) conspicuous posting of the notice on SCFHP's internet website; and 3) notification to major statewide media and the Office of Information Security within the California Technology Agency.

If the breach affects more than 500 members, SCFHP will send a single sample copy of the security breach notification to the Attorney General (excluding any personally identifiable information).

SCFHP'S POLICIES AND PROCEDURES FOR PRESERVING THE CONFIDENTIALITY OF MEDICAL RECORDS ARE AVAILABLE AND WILL BE FURNISHED TO YOU UPON REQUEST.

How Do You Contact Us to Use Your Rights?

If you want to use any of the privacy rights explained in this notice, please call or write us at:

Compliance and Privacy Officer
Santa Clara Family Health Plan
PO Box 18880
San Jose, CA 95158

Toll-free: **1-800-260-2055**
Fax: **1-408-874-1970**
TTY/TDD: **711**

Complaints

If you believe that we have not protected your privacy and wish to complain, you may file a complaint (or grievance) by calling or writing us:

Attn: Compliance and Privacy Officer
Santa Clara Family Health Plan
PO Box 18880
San Jose, CA 95158

Toll-free: **1-800-260-2055**
Fax: **1-408-874-1970**
TTY/TDD: **711**

OR you may contact the agencies below:

Privacy Office Hotline/Office of HIPAA Compliance (OHC)
Phone: **1-916-445-4646**
Toll-free: **1-866-866-0602**
Email: **privacyofficer@dhcs.ca.gov**

Attn: Regional Manager
Office for Civil Rights
U.S. Department of Health and Human Services
90 7th St, Ste 4-100
San Francisco, CA 94103
Customer Response Center: **1-800-368-1019**
Fax: **1-202-619-3818**
TDD: **1-800-537-7697**
Email: **ocrmail@hhs.gov**

Use Your Rights Without Fear

We cannot take away your health care benefits or do anything to hurt you in any way if you file a complaint or use any of the privacy rights in this notice.

Questions

If you have any questions about this notice and want further information, please contact the SCFHP Privacy Officer at the address and phone number above. To get a copy of this notice in other languages, braille, large print, on audiocassette or CD-ROM, please call or write the SCFHP Privacy Officer at the number or address listed on page 7.