

## NOTICE OF PRIVACY PRACTICES

Gilchrist Aesthetic and Medical Dermatology  
345 Saxony Road, Suite 201  
Encinitas, CA 92024  
Privacy Officer: Deborah McBride, 760-230-2537  
**Effective Date: 01/26/13**

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.

*We understand the importance of privacy and are committed to maintaining the confidentiality of your medical information. We make a record of the medical care we provide and may receive such records from others. We use these records to provide or enable other health care providers to provide quality medical care, to obtain payment for services provided to you as allowed by your health plan and to enable us to meet our professional and legal obligations to operate this medical practice properly. We are required by law to maintain the privacy of protected health information and to provide individuals with notice of our legal duties and privacy practices with respect to protected health information. This notice describes how we may use and disclose your medical information. It also describes your rights and our legal obligations with respect to your medical information. If you have any questions about this Notice, please contact our Privacy Officer listed above.*

### TABLE OF CONTENTS

A. How This Medical Practice May Use or Disclose Your Health Information	p. 2
B. When This Medical Practice May Not Use or Disclose Your Health Information	p. 5
C. Your Health Information Rights	p. 5
1. Right to Request Special Privacy Protections	
2. Right to Request Confidential Communications	
3. Right to Inspect and Copy	
4. Right to Amend or Supplement	
5. Right to an Accounting of Disclosures	
6. Right to a Paper Copy of this Notice	
D. Changes to this Notice of Privacy Practices	p. 6
E. Complaints	p. 6

## **A. How This Medical Practice May Use or Disclose Your Health Information**

This medical practice collects health information about you and stores it in a chart and on a computer. This is your medical record. The medical record is the property of this medical practice, but the information in the medical record belongs to you. The law permits us to use or disclose your health information for the following purposes:

- 1. Treatment.** We use medical information about you to provide your medical care. We disclose medical information to our employees and others who are involved in providing the care you need. For example, we may share your medical information with other physicians or other health care providers who will provide services which we do not provide. Or we may share this information with a pharmacist who needs it to dispense a prescription to you, or a laboratory that performs a test. We may also disclose medical information to members of your family or others who can help you when you are sick or injured.
- 2. Payment.** We use and disclose medical information about you to obtain payment for the services we provide. For example, we give your health plan the information it requires before it will pay us. We may also disclose information to other health care providers to assist them in obtaining payment for services they have provided to you.
- 3. Health Care Operations.** We may use and disclose medical information about you to operate this medical practice. For example, we may use and disclose this information to review and improve the quality of care we provide, or the competence and qualifications of our professional staff. Or we may use and disclose this information to get your health plan to authorize services or referrals. We may also use and disclose this information as necessary for medical reviews, legal services and audits, including fraud and abuse detection and compliance programs and business planning and management. We may also share your medical information with our "business associates," such as our billing service, that perform administrative services for us. We have a written contract with each of these business associates that contains terms requiring them to protect the confidentiality and security of your medical information. Although federal law does not protect health information which is disclosed to someone other than another healthcare provider, health plan or healthcare clearinghouse, under California law all recipients of health care information are prohibited from redisclosing it except as specifically required or permitted by law. We may also share your information with other health care providers, health care clearinghouses or health plans that have a relationship with you, when they request this information to help them with their quality assessment and improvement activities, their efforts to improve health or reduce health care costs, their review of competence, qualifications and performance of health care professionals, their training programs, their accreditation, certification or licensing activities, or their health care fraud and abuse detection and compliance efforts.
- 4. Appointment Reminders.** We may use and disclose medical information to contact and remind you about appointments. If you are not home, we may leave this information on your answering machine or in a message left with the person answering the phone.
- 5. Sign In Sheet.** We may use and disclose medical information about you by having you sign in when you arrive at our office. We may also call out your name when we are ready to see you.
- 6. Notification and Communication With Family.** We may disclose your health information to notify or assist in notifying a family member, your personal representative or another person responsible for your care about your location, your general condition or in the event of your death. In the event of a disaster, we may disclose information to a relief organization so that they may coordinate these notification efforts. We may also disclose information to someone who is involved with your care or

helps pay for your care. If you are able and available to agree or object, we will give you the opportunity to object prior to making these disclosures, although we may disclose this information in a disaster even over your objection if we believe it is necessary to respond to the emergency circumstances. If you are unable or unavailable to agree or object, our health professionals will use their best judgment in communication with your family and others.

**7. Marketing.** We may contact you to give you information about products or services related to your treatment, case management or care coordination, or to direct or recommend other treatments or health-related benefits and services that may be of interest to you, or to provide you with small gifts. We may also encourage you to purchase a product or service when we see you. If you are currently an enrollee of a health plan, we may receive payment for communications to you in conjunction with our provision, coordination, or management of your health care and related services, including our coordination or management of your health care with a third party, our consultation with other health care providers relating to your care, or if we refer you for health care, but only to the extent these communications describe: 1) a provider's participation in the health plan's network, 2) the extent of your covered benefits, or 3) concerning the availability of more cost-effective pharmaceuticals. We will not accept any payment for other marketing communications without your prior written authorization unless you have a chronic and seriously debilitating or life-threatening condition and we are making the communication in conjunction with our provision, coordination, or management of your health care and related services, including our coordination or management of your health care with a third party, our consultation with other health care providers relating to your care, or if we refer you for health care. If we make these types of communications to you while you have a chronic and seriously debilitating or life-threatening condition, we will tell you who is paying us, and we will also tell you how to stop these communications if you prefer not to receive them. We will not otherwise use or disclose your medical information for marketing purposes without your written authorization, and we will disclose whether we receive any payments for any marketing activity you authorize.

**8. Required by Law.** As required by law, we will use and disclose your health information, but we will limit our use or disclosure to the relevant requirements of the law. When the law requires us to report abuse, neglect or domestic violence, or respond to judicial or administrative proceedings, or to law enforcement officials, we will further comply with the requirement set forth below concerning those activities.

**9. Public Health.** We may, and are sometimes required by law to disclose your health information to public health authorities for purposes related to: preventing or controlling disease, injury or disability; reporting child, elder or dependent adult abuse or neglect; reporting domestic violence; reporting to the Food and Drug Administration problems with products and reactions to medications; and reporting disease or infection exposure. When we report suspected elder or dependent adult abuse or domestic violence, we will inform you or your personal representative promptly unless in our best professional judgment, we believe the notification would place you at risk of serious harm or would require informing a personal representative we believe is responsible for the abuse or harm.

**10. Health Oversight Activities.** We may, and are sometimes required by law to disclose your health information to health oversight agencies during the course of audits, investigations, inspections, licensure and other proceedings, subject to the limitations imposed by federal and California law.

**11. Judicial and Administrative Proceedings.** We may, and are sometimes required by law, to disclose your health information in the course of any administrative or judicial proceeding to the extent expressly authorized by a court or administrative order. We may also disclose information about you in response to a subpoena, discovery request or other lawful process if reasonable efforts have been made to notify you

of the request and you have not objected, or if your objections have been resolved by a court or administrative order.

**12. Law Enforcement.** We may, and are sometimes required by law, to disclose your health information to a law enforcement official for purposes such as identifying or locating a suspect, fugitive, material witness or missing person, complying with a court order, warrant, grand jury subpoena and other law enforcement purposes.

**13. Coroners.** We may, and are often required by law, to disclose your health information to coroners in connection with their investigations of deaths.

**14. Organ or Tissue Donation.** We may disclose your health information to organizations involved in procuring, banking or transplanting organs and tissues.

**15. Public Safety.** We may, and are sometimes required by law, to disclose your health information to appropriate persons in order to prevent or lessen a serious and imminent threat to the health or safety of a particular person or the general public.

**16. Specialized Government Functions.** We may disclose your health information for military or national security purposes or to correctional institutions or law enforcement officers that have you in their lawful custody.

**17. Worker's Compensation.** We may disclose your health information as necessary to comply with worker's compensation laws. For example, to the extent your care is covered by workers' compensation, we will make periodic reports to your employer about your condition. We are also required by law to report cases of occupational injury or occupational illness to the employer or workers' compensation insurer.

**18. Change of Ownership.** In the event that this medical practice is sold or merged with another organization, your health information/record will become the property of the new owner, although you will maintain the right to request that copies of your health information be transferred to another physician or medical group.

**19. Breach Notification.** In the case of a breach of unsecured protected health information, we will notify you as required by law. If you have provided us with a current email address, we may use email to communicate information related to the breach. In some circumstances our business associate may provide the notification. We may also provide notification by other methods as appropriate.

**20. Research.** We may disclose your health information to researchers conducting research with respect to which your written authorization is not required as approved by an Institutional Review Board or privacy board, in compliance with governing law.

## **B. When This Medical Practice May Not Use or Disclose Your Health Information**

Except as described in this Notice of Privacy Practices, this medical practice will not use or disclose health information which identifies you without your written authorization. If you do authorize this medical practice to use or disclose your health information for another purpose, you may revoke your authorization in writing at any time.

## **C. Your Health Information Rights**

**1. Right to Request Special Privacy Protections.** You have the right to request restrictions on certain uses and disclosures of your health information by a written request specifying what information you want to limit, and what limitations on our use or disclosure of that information you wish to have imposed. If you tell us not to disclose information to your commercial health plan concerning health care items or services for which you paid for in full out-of-pocket, we will abide by your request, unless we must disclose the information for treatment or legal reasons. We reserve the right to accept or reject any other request, and will notify you of our decision.

**2. Right to Request Confidential Communications.** You have the right to request that you receive your health information in a specific way or at a specific location. For example, you may ask that we send information to a particular e-mail account or to your work address. We will comply with all reasonable requests submitted in writing which specify how or where you wish to receive these communications.

**3. Right to Inspect and Copy.** You have the right to inspect and copy your health information, with limited exceptions. To access your medical information, you must submit a written request detailing what information you want access to and whether you want to inspect it or get a copy of it. We will charge a reasonable fee, as allowed by California and federal law. We may deny your request under limited circumstances. If we deny your request to access your child's records or the records of an incapacitated adult you are representing because we believe allowing access would be reasonably likely to cause substantial harm to the patient, you will have a right to appeal our decision. If we deny your request to access your psychotherapy notes, you will have the right to have them transferred to another mental health professional. If your written request clearly, conspicuously and specifically asks us to send you or some other person or entity an electronic copy of your medical record, and we do not deny the request as discussed above, we will send a copy of the electronic health record as you requested, and will charge you no more than what it costs us to respond to your request.

**4. Right to Amend or Supplement.** You have a right to request that we amend your health information that you believe is incorrect or incomplete. You must make a request to amend in writing, and include the reasons you believe the information is inaccurate or incomplete. We are not required to change your health information, and will provide you with information about this medical practice's denial and how you can disagree with the denial. We may deny your request if we do not have the information, if we did not create the information (unless the person or entity that created the information is no longer available to make the amendment), if you would not be permitted to inspect or copy the information at issue, or if the information is accurate and complete as is. You also have the right to request that we add to your record a statement of up to 250 words concerning any statement or item you believe to be incomplete or incorrect.

**5. Right to an Accounting of Disclosures.** You have a right to receive an accounting of disclosures of your health information made by this medical practice, except that this medical practice does not have to account for the disclosures provided to you or pursuant to your written authorization, or as described in

paragraphs 1 (treatment), 2 (payment), 3 (health care operations), 6 (notification and communication with family) and 16 (specialized government functions) of Section A of this Notice of Privacy Practices or disclosures for purposes of research or public health which exclude direct patient identifiers, or which are incident to a use or disclosure otherwise permitted or authorized by law, or the disclosures to a health oversight agency or law enforcement official to the extent this medical practice has received notice from that agency or official that providing this accounting would be reasonably likely to impede their activities.

**6. You have a right to a paper copy of this Notice of Privacy Practices**, even if you have previously requested its receipt by e-mail. If you would like to have a more detailed explanation of these rights or if you would like to exercise one or more of these rights, contact our Privacy Officer listed at the top of this Notice of Privacy Practices.

#### **D. Changes to this Notice of Privacy Practices**

We reserve the right to amend this Notice of Privacy Practices at any time in the future. Until such amendment is made, we are required by law to comply with this Notice. After an amendment is made, the revised Notice of Privacy Protections will apply to all protected health information that we maintain, regardless of when it was created or received. We will keep a copy of the current notice posted in our reception area, and a copy will be available at each appointment. We will also post the current notice on our website.

#### **E. Complaints**

Complaints about this Notice of Privacy Practices or how this medical practice handles your health information should be directed to our Privacy Officer listed at the top of this Notice of Privacy Practices. If you are not satisfied with the manner in which this office handles a complaint, you may submit a formal complaint to:

Region IX  
Office for Civil Rights  
U.S. Department of Health & Human Services  
90 7th Street, Suite 4-100  
San Francisco, CA 94103  
(415) 437-8310; (415) 437-8311 (TDD)  
(415) 437-8329 FAX  
[OCRMail@hhs.gov](mailto:OCRMail@hhs.gov)

The complaint form may be found at [www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaint.pdf](http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaint.pdf).

You will not be penalized for filing a complaint.

## **Updates to Our HIPAA Policy in Compliance with the New HIPAA Omnibus Final Rule that modified the HITECH Act and Rules, effective March 26, 2013.**

### **Business Associate Agreements**

All vendors with whom we do business (our Business Associates (BAs)) who create, receive, maintain, or transmit PHI on Gilchrist Aesthetic and Medical Dermatology's ("GAMD's" "our") behalf must have signed Business Associate Agreements (BAAs) on file. Our BAs include but are not limited to:

our electronic health record vendor  
our electronic prescribing vendor  
our medical billing company  
the lab that processes our histopathology specimens  
our Information Technology support team

Entities that are exempt from BA status are other healthcare providers, insurance plans, government agencies, and conduits who provide very temporary storage of PHI (e.g., United Parcel Service, United States Postal Service, FedEx, our Internet Service Provider).

BAs can only use and disclose PHI as permitted by the BAA or as required by law. The BA has direct liability for impermissible use/disclosure of PHI, failure to provide notifications of breach to GAMD, failure to provide access to GAMD or a patient to copy electronic PHI, failure to disclose PHI when required by the department of Health and Human Services (HHS) for an investigation, failure to provide accounting of disclosures to GAMD for GAMD's compliance with the law, failure to comply with the Security Rule administrative, physical, and technical standards, and failure to enter into BAAs with subcontractors.

### **Breach**

A "breach" of PHI is the acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy rule which compromises the security or privacy of the PHI. If a breach is suspected, GAMD is required to perform a risk assessment to determine the probability that the PHI has been compromised. If a breach is likely, notifications are required. Notifications may also be made without a risk assessment. Notifications are not required upon impermissible use/disclosure of properly encrypted PHI.

Unless a risk assessment demonstrates a low probability of compromise to the PHI, breach notifications must be made. There is a standard four-factor risk assessment:

1. What is the nature and extent of PHI involved in the breach including types of identifiers and likelihood of re-identification?
2. Who was the unauthorized person to whom disclosure was made or who used the information?
3. Was the PHI actually acquired or viewed?
4. What is the extent to which the risk to the PHI has been mitigated?

### **Patients' Right to Access PHI**

Patients have the right to request an electronic copy of all electronic data, whether in one or more data sets. GAMD must provide data in the format requested by the individual. Any linked images or other data must be included. Data may be transmitted unencrypted if the individual consents. Data that GAMD or a BA maintains off-site is subject to the same rules. A reasonable cost-based fee may be charged to the individual to produce a copy of PHI.

**Updates to Our HIPAA Policy in Compliance with the New HIPAA Omnibus Final Rule that modified the HITECH Act and Rules, effective March 26, 2013. (continued)**

**Patient's Right to Restrict Disclosure**

Patients can request disclosure not be made to health insurance plans if 1) the disclosure is for payment of health-care operations and not otherwise required by law, and 2) the restriction is solely for an item or service for which the patient paid in full. GAMD may require payment in full at the time of service or purchase. For bundled services, GAMD may inform the patient of our inability to restrict disclosure on one item only. Contractual obligations to HMOs do not exempt GAMD from this rule. The patient is responsible for notifying downstream providers of their wish to restrict disclosure.