

NOTICE OF PRIVACY PRACTICES-IT'S A SECRET MED SPA

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.

If you have any questions about this Notice, please contact our Privacy Officer at the telephone number or email address listed at the end of this Notice.

Each time you visit a healthcare provider, a record of your care is created. Typically, this record contains medical information such as your symptoms, examination, test results, diagnoses, treatment and/or treatment plan and billing-related information. This information is considered protected health information (PHI).

This Notice is intended to advise you about the ways we may use and disclose medical information about you and comply with the Health Insurance Portability and Accountability Act (HIPAA). It also describes your rights and certain obligations with regard to your medical information and applies to all of the records of your care generated by your healthcare provider(s) for our organization.

Our Responsibilities

It's A Secret Med Spa and/or its subsidiaries and/or affiliates, ("Company") is required to maintain the privacy of your health information and to provide you with a description of our legal duties and privacy practices regarding your health information that we collect and maintain.

We are required by law to abide by the terms of this Notice and notify you if changes are made. We reserve the right to make changes to the Notice and make the new provisions effective for all protected health information we maintain. Copies of our Notice is provided electronically to each patient and is available in printed copy at each location and on our website.

How We May Use and Disclose Medical Information about You

The following describes examples of the way we may use and disclose medical information:

For Treatment: We may use medical information about you to provide, coordinate and manage your treatment or services. We may disclose medical information about you to other healthcare professionals such as physicians, nurses, or other personnel who are involved in your care.

We may communicate your information using various methods, orally, written, or via electronic communications.

We may also provide other healthcare professionals who contribute to your care with copies of your information to assist him/her and ensure that they have appropriate information regarding your condition/treatment plan and diagnosis.

For Payment: We may use and disclose medical information about your treatment/services to bill and collect payment from a third-party financial vendor(s). Examples may include contacting CareCredit or similar vendor(s) for authorization/preapproval of covered services.

For Health Care Operations: We may use or disclose, as needed, your health information in order to support our business activities. These activities may include, but are not limited to quality assessments, employee review activities, licensing, legal advice, accounting support, information systems support and conducting or arranging other business activities. We may contact you to remind you of your appointment by telephone, email or text messaging unless requested otherwise.

Business Associates, BA: Provide services for our organization through written contracts and/or service agreements. Examples of these services include third-party financial vendors and software support. We may disclose your health information to a BA so they can perform the services we have asked them to do such as provide financial services for services rendered. The BA is also required by law to protect and safeguard your health information which is clearly defined through our Business Associate Agreement and written contracts/service agreements.

Breach Notification: In the event that there has been a breach of unsecured protected health information (PHI) identified on behalf of our organization or a BA you will be notified within 60 days of the breach. In addition to your individual notification we may be required to meet further reporting requirements set forth by state and federal agencies.

Uses and Disclosures That May Be Made *With Your Consent, Authorization or Opportunity to Object*

We will not use and disclose information without your written authorization, except as described in this Notice or as required by applicable laws. Written authorization is required for, most uses and disclosures of PHI, PHI for marketing purposes unless we speak

with you and disclosures that constitute a sale of PHI. If you provide an authorization to use or disclose medical information about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. However, we are unable to take back any disclosures we have already made with your authorization.

Individuals Involved in Your Care: Unless you object, we may release medical information about you to a friend or family member who is involved in your treatment.

Future Communications: We may communicate with you via newsletters, mailings or other means regarding treatment options and information on health-related benefits or services; to remind you that you have an appointment; or other community-based initiatives or activities to include limited marketing or vendor events in which our location(s) are participating. You have the right to opt out at any time if you are not interested in receiving these communications, please contact our Privacy Officer if you are unable to opt out.

Marketing and Fundraising initiatives, if applicable are limited and may require a separate authorization.

Uses and Disclosures That May Be Made *Without Your Authorization or Opportunity to Object*

We may use or disclose your health information in the following situations without your authorization or without providing you with an opportunity to object. These situations include:

As required by law: We may use and disclose health information to the following types of entities, including but not limited to:

- Food and Drug Administration
- Public Health or Legal Authorities charged with preventing or controlling disease, injury or disability
- Correctional Institutions
- Workers Compensation Agents
- Organ and Tissue Donation Organizations
- Military Command Authorities
- Health Oversight Agencies
- Funeral Directors, Coroners and Medical Directors
- National Security and Intelligence Agencies
- Protective Services for the President and Others
- Authority that receives reports on abuse and neglect

If you are not present, able to agree or object to the use or disclosure (such as in an emergency situation), then your healthcare provider may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the information that is relevant to your health care will be disclosed.

Law Enforcement/Legal Proceedings: We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena or court order.

State-Specific Requirements: Many states have reporting requirements which may include population-based activities relating to improving health or reducing health care costs, cancer registries, birth defect registries and others.

Your Health Information Rights

Although your health record is the physical property of the organization that compiled it, you have the right to:

Inspect and Copy: You and/or your personal representative have the right to inspect, review and receive a copy of your medical information. Electronic copies are available and may include various electronic means such as a patient portal or other reasonable accommodations requested. We may deny your request to inspect and copy in limited circumstances to include release of psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. If you are denied access to medical information, you may request that the denial be reviewed.

Requests to copy and/or a review must be submitted in writing to Company. There will be no fee charged for applicable copying and/or producing copy of portable media (USB) up to the maximum amount as prescribed by governing law.

Amend: If you feel that the medical information, we have is incomplete or incorrect, you may ask us to amend the information by submitting a request in writing to the Privacy Officer providing a reason to support the amendment request. You will be notified of the decision of your request in writing within 60 days.

An Accounting of Disclosures: You have the right to request an accounting of our disclosures of your medical information; the list will not include disclosures to carry out treatment, payment and health care operations. Company will provide the first accounting to you in any 12-month period without charge, upon receipt of your written request. The cost for subsequent requests for an accounting within the 12-month period will be up to the maximum amount prescribed by governing law.

Request Restrictions: You have the right to request a restriction or limitation of your medical information we use or disclose about you for treatment, payment or health care operations. **Other Restrictions, Limiting Information:** You also have the right to request and limit any medical information we disclose about you to someone you have approved, such as a friend or family member that is involved in your treatment. We ask that you submit these requests in writing.

We may not agree or be required to agree to your request(s) for specific reasons, if this occurs, you will be informed of the reason(s) for the denial.

Request Confidential Communications: You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. We will agree to the request to the extent that it is reasonable for us to do so. For example, you may request that we contact you by using an alternate phone number or email/ mailing address. We ask that you submit these requests in writing.

E-mail communication requests if applicable may require a separate authorization.

To exercise any of your rights, please submit your request in writing to the organization's privacy officer listed below.

For More Information or to Report a Problem

If you have questions and would like additional information, please contact the Privacy Officer. If you believe that your (or someone else's) privacy rights may have been violated, you may file a complaint with the Privacy Officer at the contact number below or with the Secretary of Health and Human Services at 800-368-1019. Further instructions for filing a complaint can also be found at www.hhs.gov/ocr. All complaints must be submitted in writing within 180 days of when you knew that the act or omission occurred and there will be no retaliation for filing a complaint.

Privacy Officer: General Counsel

Corporate Office: It's A Secret Med Spa

Telephone Number: 469-639-2011

104 Decker Drive, Suite 200

Email address: compliance@secretmedspa.com

Irving, Texas 75062

Effective Date: September 1, 2016 rev. 04.01.23