

## **HIPAA Notice of Privacy Practices (OMNIBUS Rule) for the practice of:**

Renewal Dermatology & MedSpa located at:

7512 Gardner Park Drive, Gainesville, VA 20155

1850 Town Center Pkwy, Pavilion II Suite 360, Reston, VA 20190

8650 Sudley Road, Suite 310, Manassas, VA 20110 // 10680 Crestwood Drive, Manassas, VA 20109

8136 Old Keene Mill Road, Suite A201, Springfield, VA 22152

11096 Lee Highway, Suite B102, Fairfax, VA 22030

13 West Main St., Berryville, VA 22611

---

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION under the HIPAA Omnibus Rule of 2013.

### **Please review the following carefully:**

For the purpose of this Notice “us”, “we” and “our” refers to the name of this practice: Renewal Dermatology & MedSpa and “you” or “your” refers to our patients (or their legal representatives as determined by us in accordance with state informed consent law). When you receive healthcare services from us, we will obtain access to your medical information. We are committed to maintaining the privacy of your health information and have implemented numerous procedures to ensure that we do so.

The federal Health Insurance Portability & Accountability Act of 2013, HIPAA Omnibus Rule (formerly HIPAA 1996 & HITECH of 2009) require us to maintain the confidentiality of all your healthcare records and other identifiable patient information (PHI) used by or disclosed to us in any form, whether electronic, on paper, or spoken. HIPAA is a federal law that gives you significant new rights to understand and control how your health information is used. Federal and state laws provide penalties for covered health entities, business associates and subcontractors that misuse or improperly disclose PHI.

HIPAA requires us to provide you with the Notice of our legal duties and the privacy practices we are required to follow when you first come into our office for healthcare services. If you have any questions, please speak to our Privacy Practices Officer.

Our doctors, clinical staff, administrative staff, and business associates (including their subcontractors) all follow the policies and procedures set forth in this Notice.

### **OUR RULES ON HOW WE MAY USE AND DISCLOSE YOUR PHI**

Under the law, we must have your signature on a written, dated Authorization Form of Acknowledgment of this Notice (referred to as “AoA” in this Notice), before we will use or disclose your PHI for certain purposes as detailed in the rules below:

1. Documentation: You will be asked to sign an AoA form when you receive this Notice of Privacy Practices. If you did not sign such a form or need a copy of the one you signed, please contact our privacy officer. You may revoke your consent at any time (unless we already have acted based on it) by submitting our Revocation Form in writing to us at our address listed above (it will take effect when we actually receive it). It will not affect any use or disclosure that occurred prior to the revocation.
2. General Rule: If you do not sign our AoA, or you revoke it, as a general rule, we can only use or disclose to anyone (except you) your PHI or any information in your medical record as HIPAA permits or requires. We are unable to submit claims to payers under assignment of benefits without your signature on our AoA form. You can restrict disclosure to your insurance company for any services you pay for ‘out of pocket’ under the 2013 Omnibus Rule. We will not condition treatment on you signing an AoA, but we may be forced to decline you as a new patient or discontinue you as an active patient if you choose not to sign the AoA or you revoke it.

### **HEALTHCARE TREATMENT, PAYMENT AND OPERATIONS RULE**

With your signed consent (on our AoA), we may use or disclose your PHI in order:

- To provide you with or coordinate healthcare treatments and services. For example, this includes consulting with other doctors about your care, delegating tasks to ancillary staff, calling in prescriptions to your pharmacy, disclosing

information to family or others so that they may assist you with home care, arrange appointments with other providers, schedule ancillary testing or lab work for you, etc.

- To bill or collect payment from you, an insurance company, a managed care organization, a health benefit plan or another 3<sup>rd</sup> party.
- To run our office, assess the quality of care our patients receive and provide you with customer service. For example, this includes contacting you to remind you of appointments or missed appointments, we may leave messages (not giving out detailed PHI) with whoever answers your phone or on your answering machine, etc.
- The HIPAA Omnibus Rule does not require that we provide the above notice of “Healthcare Treatment, Payment and Operations Rule” but we are including it as a courtesy, so that you may understand our use of your PHI with our business practices.
- FYI: Under the Omnibus Rule, health insurance plans cannot use or disclose genetic information for underwriting purposes.

#### **SPECIAL RULES**

Notwithstanding anything else contained in this notice, only in accordance with applicable HIPAA Omnibus Rule, under strictly limited circumstances, we may use or disclose your PHI without your permission, consent or authorization for the following purposes:

- When required under federal, state or local law.
- When necessary for public health reasons (i.e. disease control, disability, adverse reactions to medications, etc).
- When necessary in emergencies to prevent a serious threat to your health/safety of other persons.
- For federal or state government healthcare oversight activities.
- For judicial and administrative proceedings and law enforcement purposes.
- For Workers Compensation purposes.
- For organ or tissue donation.
- For research projects approved by an Institutional Review Board or a privacy board.
- To family members, friends and other persons identified by you as involved in your healthcare or payment related to your healthcare, if you are present and give permission. This includes, if you bring someone into the exam room or conference area where we are discussing your PHI. We may disclose the minimum necessary PHI without your explicit permission, consent or authorization, if, e.g., we reasonably infer that it is in your best interest to allow a person to act on your behalf who knows you are a patient and was asked by you to pick up records, DME, or prescriptions. Or, if it is an emergency situation involving you and we determine it is in your best interest to disclose your PHI, in which case only pertinent information will be disclosed and you will be notified as soon as possible. As per HIPAA law 164.512(j) if disclosure: (A) is necessary to prevent or lessen a serious imminent threat to the health and safety of a person or the public and (B) is made to a person or persons reasonably able to prevent or lessen that threat.

#### **MINIMUM NECESSARY RULE**

Our staff will not use or access your PHI unless it is needed to do their jobs. All of our team members are trained in HIPAA Privacy rules and sign a strict Confidentiality Contract with regards to keeping your PHI. So do our Business Associates and subcontractors. Also we disclose to outside staff, only as much of your PHI as is needed to accomplish the recipient’s lawful purposes. Still in certain cases, we may use and disclose the entire contents of your entire medical record:

- To you (or legal representatives as stated above) and anyone else you list on your AoA to receive a copy of your records.
- To healthcare providers for treatment purposes (this includes referrals to other doctors or reports requested by another of your doctors).
- To the US Dept of Health and Human Services.
- To others required as required under federal and state law.
- To our privacy officer and others as needed to resolve a complaint or accomplish your request under HIPAA. In accordance with HIPAA law, we presume that requests for disclosure of PHI from another Covered Entity (as defined in HIPAA) are for the minimum necessary amount of PHI to accomplish the requestor’s purposes. Our privacy officer determines “minimum necessary” to disclose based on the following:
  - Amount of information being disclosed
  - Number of individuals or entities to whom it is being disclosed

- Importance of use or disclosure
- Likelihood of further disclosure
- Whether the same result can be achieved with 'de-identified' information
- Technology available to protect confidentiality of information
- Cost to implement administrative, technical and security procedures to protect confidentiality.
- If we believe a request is unclear, or we feel is not needed, we will ask the requester to document why this is needed.

#### **INCIDENTAL DISCLOSURE RULE**

We will take reasonable administrative, technical and security safeguards to ensure the privacy of your PHI when we use or disclose it. We use a firewall and a router to federal standards, change passwords periodically, backup our PHI data offsite and do not allow unauthorized access to areas where PHI is stored.

In the event that there is a breach in protecting your PHI, we will follow Federal Guidelines to HIPAA Omnibus Rule Standard to first evaluate the breach situation using the Omnibus Rule, 4-Factor Formula for Breach Assessment. Then we will document the situation, retain copies of the situation on file, and report all breaches (other than low probability, as described by the Omnibus Rule) to the US Dept of Health and Human Services. We will also notify you and other parties of significance as required by HIPAA Law.

#### **BUSINESS ASSOCIATE RULE**

Business associates are defined as: an entity, which in the course of their work will directly or indirectly use, transmit, view, transport, hear, interpret process or offer PHI for this Facility. Business associates and other 3<sup>rd</sup> parties that receive your PHI from us will be prohibited from re-disclosing that information. Business associates are required to sign a Confidentiality Agreement to Federal Omnibus Standards and follow Omnibus rules.

#### **SUPER-CONFIDENTIAL INFORMATION RULE**

If we have PHI about you regarding communicable disease, disease testing, alcohol or substance abuse diagnosis and treatment, or mental health records (super-confidential information under the law), we will not disclose it under the General or Healthcare Treatment, Payment, Operations Rules without your first signing and properly completing your AoA form. If we disclose super-confidential information, we will comply with federal laws that require us to warn the recipient that re-disclosure is prohibited.

#### **CHANGES TO PRIVACY RULES**

We reserve the right to change our privacy practices at any time as authorized by law. The changes will be considered immediate and will apply to all PHI we create or receive in the future. If we make changes, we will post the changed notice in our office. Upon request, you will be given a copy of our current notice.

#### **AUTHORIZATION RULE**

We will not use or disclose your PHI for any purpose other than as stated in the Notice above without your signature for consent.

#### **MARKETING RULES**

Marketing is defined as communication about a product or service that encourages recipients to purchase or use the product or service. Under the HIPAA Omnibus Rule, we have included a section on our AoA to obtain your authorization. In general, we use marketing to inform you about products, services, or new technology that can benefit you as well as current patient appreciation sales/specials.

#### **FUNDRAISING RULES**

We do not participate in fundraising with our patient information.

#### **AUTHORIZATIONS RELATED TO RESEARCH**

We may seek authorizations from you for the use of your PHI for future research. However, we would make clear the research it is being used for. As of Dec. 13, 2016, HIPAA permits disclosure of your PHI for research related to quality, safety, or effectiveness of a product regulated by the FDA.

#### **YOUR RIGHTS REGARDING YOUR PHI**

If you got this notice via email or website, you have the right to a paper copy by asking our privacy officer. You also have the right to see and get a copy of your PHI by submitting a request to our privacy officer or filling out a record request form. We may

charge a fee for the copy, not to exceed \$25. And we may charge a mailing fee if a paper copy is requested via mail, not to exceed \$10. We will respond with a copy within 30 days as required by federal law.

#### **REQUEST FOR CORRECTION TO PHI**

If we receive a correction to your PHI via another doctor or you, we will make the changes upon receipt of written notification. You may request a correction to your PHI by filling out a request for Amendment/Correction form. We will act upon your request within 30 days. We will make the changes by noting, not deleting, and notify you within 5 days that the corrections have been made. We may deny your request under certain circumstances. If we do, we will notify you in writing within 5 business days.

#### **TO REQUEST RESTRICTIONS**

You may ask us to limit how your PHI is used and disclosed by submitting a written Request for Restriction on Use/ Disclosure to our Privacy Officer. We will consider each request; but, are not required to agree to a restriction except in case of a request restricting disclosure to a health plan for the purpose of carrying out payment or health care operations when disclosure is not mandated by law, and the PHI pertains solely to a health care item or service for which you or another person other than the health plan, has paid the covered entity in full . For instance, we would be unable to grant a request if the PHI use/ disclosure is required by law, your care was provided during an emergency situation without time to check limitations, or your request would, in our professional judgement, not be aligned with our mutual best interests.

#### **TO REQUEST ALTERNATIVE COMMUNICATIONS**

You may ask us to communicate with you in a different way or at a different place by submitting a written request for Alternative Communication form to us. We will accommodate all reasonable requests.

#### **COMPLAINTS OR TO GET MORE INFORMATION**

We will follow the rules set forth in this Notice. If you want more information, or if you believe your privacy rights have been violated, we want to make it right. We never penalize you for filing a complaint. To do so, please file a formal written complaint within 180 days to our Privacy Officer at: *Renewal Dermatology & MedSpa, attn: Nicole Hoffman, 7512 Gardner Park Drive, Gainesville, VA 20155*.(ph: 703.753.9860) Or you may contact DHHS at: *Office of Civil Rights, 200 Independence Ave SW, Washington, DC 20201*.

These privacy practices are in accordance with the original HIPAA enforcement effective April 14, 2003 and updated to the Omnibus Rule effective March 26<sup>th</sup>, 2013 and will remain in effect until we replace them as specified by Federal and State law.

#### **FAXING, EMAILING AND TEXTING RULE**

When you request us to fax, email or text your PHI as an alternative communication, we may agree to do so, but this may be reviewed by our Privacy Officer or treating doctor. By providing us with this information, you are guaranteeing that you have sole access to the fax, email or phone with text. We are not responsible for PHI viewed by others if it is a shared fax, email or phone, as you requested that it be sent there. We will include a cover letter and attach appropriate notice to the message.

#### **PRACTICE TRANSITION RULE**

IF we sell our practice, our patient records may be disclosed and physical custody may be transferred to the purchasing healthcare provider, but only in accordance with the law. The new record owner will be solely responsible for ensuring privacy of your PHI after the transfer and you agree that we will have no responsibility for transferred records after that. If the practice dies, our patient records will be transferred to another healthcare practitioner within 90 days or stay with the attending doctor at his/her new location. Before either of these two situations, our Privacy Officer will obtain a Business Associate Agreement from the purchaser and review your PHI.

#### **INACTIVE PATIENT RECORDS**

We will retain your records for 7 years from your last treatment or exam, at which point you will become an inactive patient in our practice and we may destroy your records at that time (inactive minor patient records will not be destroyed before their 18<sup>th</sup> birthday). We destroy them in accordance with the law.

#### **COLLECTIONS**

If we use or disclose your PHI for collection purposes, we will only do so in accordance with the law.