



Effective Date: 1/1/2020  
Last Revised: \_\_\_\_\_

## **Data Privacy - Official Policy**

### **Introduction**

Atlanta Dermatology, Vein & Research Center, LLC (dba Hamilton Dermatology) has adopted this Data Privacy-Official Policy to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act of 2009 (ARRA Title XIII). We also recognize our responsibility to protect individually identifiable health information under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under general, professional ethics.

This policy governs the designation and duties of a HIPAA Privacy-Official for Atlanta Dermatology, Vein & Research Center, LLC. All personnel of Atlanta Dermatology, Vein & Research Center, LLC must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, contractors, temporary workers, and volunteers must read, understand, and comply with this policy.

### **Assumptions**

- ❑ Atlanta Dermatology, Vein & Research Center, LLC must comply with HIPAA and the HIPAA implementing regulations concerning the designation of a Privacy Official, in accordance with the requirements at § 164.530(a).

### **Policy**

- ❑ It is the Policy of Atlanta Dermatology, Vein & Research Center, LLC to designate and always maintain an active HIPAA Privacy-Official.
- ❑ The HIPAA Privacy-Official's general responsibilities are to:
  - Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
  - Conduct various risk analyses, as needed, or required.
  - Manage breach notification investigations, determinations, and responses, including breach notifications.
  - Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.
- ❑ The HIPAA Privacy-Official's potential duties may include:
  - Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.



Effective Date: 1/1/2020  
Last Revised: \_\_\_\_\_

- Maintain an accurate inventory of (1) all individuals who have access to confidential information, including PHI, and (2) all uses and disclosures of confidential information by any person or entity.
- Administer patient requests under HIPAA's Patient Rights.
- Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with appropriate technical personnel to protect confidential information from unauthorized use or disclosure.
- Develop specific policies and procedures mandated by HIPAA.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Draft and disseminate the Privacy Notice required by the Privacy Rule.
- Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
- Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure that confidential data is adequately protected when such access is granted.
- Ensure that all policies, procedures, and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- Conduct periodic privacy audits and take remedial action as necessary.
- Oversee employee training in the areas of information privacy and security.
- Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- Remain up-to-date and advise on new technologies to protect data privacy.
- Remain up to date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- Track pending legislation regarding data privacy and if appropriate, seek to favorably influence that legislation.
- Anticipate patient or consumer concerns about our use of their confidential information and develop policies and procedures to respond to those concerns and questions.
- Evaluate privacy implications of online, web-based applications.
- Monitor data collected by or posted on our website(s) for privacy concerns.
- Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to our privacy practices.



Effective Date: 1/1/2020  
Last Revised: \_\_\_\_\_

### **Compliance and Enforcement**

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with Atlanta Dermatology, Vein & Research Center, LLC 's Sanction Policy.