

# HIPAA Security & Privacy Manual

---

Security & Privacy Officer:  
Dr. John A. Brandeisky DPM, FACFAS

Main Office:  
Freehold Office Plaza  
4249 US Highway 9 North  
Freehold, New Jersey  
07728

Satellite Office:  
Renaissance Crossings  
312 Applegarth Road  
Monroe, New Jersey  
08831

Call: 732.308.1090

Fax: 732.308.1143

eMail: [BrandeiskyOffice@gmail.com](mailto:BrandeiskyOffice@gmail.com)

Official Website: [njfootdoc.com](http://njfootdoc.com)

---

**DO NOT REMOVE THIS MANUAL FROM  
THE OFFICE!**

**YOU MAY REQUEST A COPY AND  
YOU MUST ACKNOWLEDGE RECEIPT OF  
READING OR REQUESTING A COPY OF  
THIS MANAUL OR HAVING BEEN  
OFFERED THE OPPORTUNITY TO DO SO**

.

---

---

## Quick Reference: Disclosures Requiring/Not Requiring Written Patient Authorization

---

### Disclosures Not Requiring Written Patient Authorization:

- To the patient himself/herself (Manual, Section C.1.1.1).
- To other persons/entities for purposes of the Practice's treatment, payment or health care operations (Manual, Section C.1.1.2).
- To another health care provider for that provider's treatment of the patient (Manual, Section C.1.1.3).
- To other health care providers or HIPAA "covered entities" for purposes of their making/obtaining payment for health care services (Manual, Section C.1.1.4).
- To a HIPAA "covered entity" for purposes of its health care operations (Manual, Section C.1.1.5).
- To parents of minors, guardians, conservators or other authorized representatives of the patient (Manual, Section C.2).
- To family members and/or caregivers where patient does not object verbally or where disclosure is indicated by the provider's professional judgment (Manual, Section C.3).
- To government authorities as required by law (Manual, Section C.4):

- public health reporting
- child abuse/other abuse
- domestic violence
- health oversight activities (audits, investigations)
- court orders, subpoenas, search warrants
- law enforcement (under certain circumstances)
- To government authorities or potential victims to prevent serious harm or injury (Manual, Section C.5).
- To business associates pursuant to a proper business associate agreement (Manual, Section C.6).
- For certain "research" activities (Manual, Section C.7).
- For certain "marketing" activities (Manual, Section C.7).

### Disclosures Requiring Written Patient Authorization

- All other disclosures of patient health information (Manual, Section B.2).

## **GLOSSARY OF TERMS**

**Access** – The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

**Administrative safeguards** – Administrative safeguards are the policies and procedures the Practice implements to execute the physical and technical safeguards. There are nine components of administrative safeguards in the Security Rule: (1) security management (includes performance of risk analysis, risk management, preparation of sanction policy and monitoring computer systems activities); (2) assignment of a security officer; (3) a system administrator; (4) management of the access of information; (5) security training; (6) incident reporting and investigation; (7) implementation of a contingency plan; (8) periodic evaluation of technology and upgrades; and (9) business associate agreements in place to protect ePHI.

**Authentication** – The corroboration that a person is the one claimed.

**Availability** – The property that data or information is accessible and useable upon demand by an authorized person.

**Business associate** – A person or entity who creates, receives, maintains or transmits Protected health information on behalf of a covered entity (or of an organized health care arrangement in which the covered entity participates). A business associate may assist in the performance of:

- A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- Any other function or activity regulated by HIPAA; or
- A person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity (or to or for an organized health care arrangement in which the covered entity participates) where the provision of the service involves the disclosure of individually identifiable health information from such covered entity (or arrangement), or from another business associate of such covered entity (or arrangement), to the person.
- Subcontractor of business associates are also classified as business associates,

**Confidentiality** – The property that data or information is not made available or disclosed to unauthorized persons or processes.

**Covered entity** – (1) A health plan (includes insurance companies, Medicare, Medicaid, group health plans, etc.); (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a standard HIPAA transaction (such as electronic billing).

**Disclosure** – Any release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

**Electronic media** – Includes memory devices in computers (hard drives) and any removable/transportable digital memory medium.

**Electronic Protected Health Information (ePHI)** – Individually identifiable health information transmitted by electronic media or maintained in electronic media.

**Encryption** – The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

**Facility** – The physical premises and interior and exterior of a building in which ePHI is located.

**HHS or Secretary** – The Department of Health and Human Services or the Secretary of Health and Human Services.

**Health care** – Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

**Health care provider** – A provider of services (as defined in Section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of protected health or health services (as defined in Section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

**Health information** – Any information, oral or recorded in any medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

**Individually identifiable health information** – Information that is a subset of health information, including demographic information collected from an individual, and that: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) Which identifies the individual, or (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

**Information system** – An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

**Integrity** – The property that data or information have not been altered or destroyed in an authorized manner.

**Minimum necessary** – When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

**Payment** – Any of a number of activities by a covered entity involving reimbursement or coverage related to health care or health benefits. The definition of payment includes: obtaining premiums or identifying or providing benefits under a health plan; reimbursement for health services, determining eligibility, coverage, adjudication, or subrogation of health benefit claims; risk adjusting amounts due based on enrollee health status and demographics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance and related health care data processing; review of health care services for protected health necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of certain protected health information relating to collection of premiums or reimbursement (i.e., name and address, date of birth, social security number; payment history; account number; and name and address of the health care provider and/or health plan).

**Physical safeguards** – Physical safeguards are the security measures that protect the physical facility and computer systems. There are four components of physical safeguards in the Security Rule: (1) facility access controls (locks, screen filters, magnetic cards); (2) workstation use; (3) workstation security; and (4) device and media controls (disposal, reuse, accountability and backup storage).

**Protected health information** – Individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is (1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. Protected health information excludes individually identifiable health information in employment records held by a covered entity in its role as an employer.

**Required by law** – A mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

**Security incident** – A violation of security policies and procedures. A security incident includes the attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with the operation of an information system. Examples: An unauthorized person accesses ePHI, a door is left unlocked, a hacker gets into the system. All security incidents must be documented.

**Security officer** – The individual designated by a health care provider to develop and implement security policies and procedures for the provider.

**Technical safeguards** – Technical safeguards and those electronic and computerized security measures installed (such as passwords) to protect information contained in the facility and computer system. There are five components of technical safeguards in the Security Rule: (1) access control (password encryption); (2) audit control; (3) integrity controls; (4) authorization; and (5) transmission security.

**Treatment** – The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

**Use** – With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

**Workforce** – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

**Workstation** – An electronic computing device, such as a desktop or laptop computer, personal digital assistant (PDA) or other similar electronic device.

## SUMMARY OF NOTICE OF PRIVACY PRACTICES

This summary is provided to assist you in understanding  
the attached Notice of Privacy Practices

The attached Notice of Privacy Practices contains a detailed description of how our office will protect your health information, your rights as a patient and our common practices in dealing with patient health information. Please refer to that Notice for further information.

**Uses and Disclosures of Health Information.** We will use and disclose your health information in order to treat you or to assist other health care providers in treating you. We will also use and disclose your health information in order to obtain payment for our services or to allow insurance companies to process insurance claims for services rendered to you by us or other health care providers. Finally, we may disclose your health information for certain limited operational activities such as quality assessment, licensing, accreditation and training of students.

**Uses and Disclosures Based on Your Authorization.** Except as stated in more detail in the Notice of Privacy Practices, we will not use or disclose your health information without your written authorization.

**Uses and Disclosures Not Requiring Your Authorization.** In the following circumstances, we may disclose your health information without your written authorization:

- To family members or close friends who are involved in your health care;
- For certain limited research purposes;
- For purposes of public health and safety;
- To Government agencies for purposes of their audits, investigations and other oversight activities;

- To government authorities to prevent child abuse or domestic violence;
- To the FDA to report product defects or incidents;
- To law enforcement authorities to protect public safety or to assist in apprehending criminal offenders;
- When required by court orders, search warrants, subpoenas and as otherwise required by the law.

**Patient Rights.** As our patient, you have the following rights:

- To have access to and/or a copy of your health information;
- To receive an accounting of certain disclosures we have made of your health information;
- To request restrictions as to how your health information is used or disclosed;
- To request that we communicate with you in confidence;
- To request that we amend your health information;
- To receive notice of our privacy practices.

If you have a question, concern or complaint regarding our privacy practices, please refer to the attached Notice of Privacy Practices for the person or persons whom you may contact.

### CONTACT :

JOHN BRANDEISKY DPM

PRIVACY OFFICER

4249 RT 9 NORTH

FREEHOLD NJ 07728

732-308-1090 FAX 308-1143

BRANDEISKYOFFICE@GMAIL.COM

UNSECURED E MAIL ADDRESS@RISK

\*\*\*\*\*

---

## NOTICE OF PRIVACY PRACTICES

---

**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. THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.**

---

### *Our Legal Duty*

We are required by applicable federal and state laws to maintain the privacy of your protected health information. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your protected health information. We must follow the privacy practices that are described in this notice while it is in effect. This notice takes effect August 8 2013, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all protected health information that we maintain, including medical information we created or received before we made the changes.

You may request a copy of our notice (or any subsequent revised notice) at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the information listed at the end of this notice.

### **Uses and Disclosures of Protected Health Information**

We will use and disclose your protected health information about you for treatment, payment, and health care operations.

Following are examples of the types of uses and disclosures of your protected health care information that may occur. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

**Treatment:** We will use and disclose your protected health information to provide, coordinate or manage your health care and any related services. This includes the coordination or management of your health care with a third party. For example, we would disclose your protected health information, as necessary, to a home health agency that provides care to you. We will also disclose protected health information to other physicians who may be treating you. For example, your protected health information may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you.

In addition, we may disclose your protected health information from time to time to another physician or health care provider (e.g., a specialist or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment to your physician.

**Payment:** Your protected health information will be used, as needed, to obtain payment for your health care services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you, such as: making a determination of eligibility or coverage for insurance benefits, reviewing services provided to you for protected health necessity, and undertaking utilization review activities. For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to the health plan to obtain approval for the hospital admission.

**Health Care Operations:** We may use or disclose, as needed, your protected health information in order to conduct certain business and operational activities. These activities include, but are not limited to, quality assessment activities, employee review activities, training of students, licensing, and conducting or arranging for other business activities.



For example, we may use a sign-in sheet at the registration desk where you will be asked to sign your name. We may also call you by name in the waiting room when your doctor is ready to see you. We may use or disclose your protected health information, as necessary, to contact you by telephone or mail to remind you of your appointment.

We will share your protected health information with third party “business associates” that perform various activities (e.g., billing, transcription services) for the practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

**Sale of Health Information:** We will not sell or exchange your health information for any type of financial remuneration without your written authorization.

**Fundraising Communications:** We may use or disclose your health information for fundraising purposes, but you have the right to opt-out from receiving these communications.

**Uses and Disclosures Based On Your Written Authorization:** Other uses and disclosures of your protected health information will be made only with your authorization, unless otherwise permitted or required by law as described below.

You may give us written authorization to use your protected health information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Without your written authorization, we will not disclose your health care information except as described in this notice.

**Others Involved in Your Health Care:** Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that directly relates to that person’s involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative

or any other person that is responsible for your care of your location, general condition or death.

**Marketing:** We may use your protected health information to contact you with information about treatment alternatives that may be of interest to you. We may disclose your protected health information to a business associate to assist us in these activities. If we are paid by a third party to make marketing communications to you about their products or services, we will not make such communications to you without your written authorization. Except as stated above, no other marketing communications will be sent to you without your authorization.

**Research; Death; Organ Donation:** We may use or disclose your protected health information for research purposes in limited circumstances. We may disclose the protected health information of a deceased person to a coroner, protected health examiner, funeral director or organ procurement organization for certain purposes.

**Public Health and Safety:** We may disclose your protected health information to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. We may disclose your protected health information to a government agency authorized to oversee the health care system or government programs or its contractors, and to public health authorities for public health purposes.

**Health Oversight:** We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

**Abuse or Neglect:** We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

**Food and Drug Administration:** We may disclose your protected health information to a person or company required by the Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations, to track products; to enable product recalls; to make

repairs or replacements; or to conduct post marketing surveillance, as required.

**Criminal Activity:** Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

**Required by Law:** We may use or disclose your protected health information when we are required to do so by law. For example, we must disclose your protected health information to the U.S. Department of Health and Human Services upon request for purposes of determining whether we are in compliance with federal privacy laws. We may disclose your protected health information when authorized by workers' compensation or similar laws.

**Process and Proceedings:** We may disclose your protected health information in response to a court or administrative order, subpoena, discovery request or other lawful process, under certain circumstances. Under limited circumstances, such as a court order, warrant or grand jury subpoena, we may disclose your protected health information to law enforcement officials.

**Law Enforcement:** We may disclose limited information to a law enforcement official concerning the protected health information of a suspect, fugitive, material witness, crime victim or missing person. We may disclose the protected health information of an inmate or other person in lawful custody to a law enforcement official or correctional institution under certain circumstances. We may disclose protected health information where necessary to assist law enforcement officials to capture an individual who has admitted to participation in a crime or has escaped from lawful custody.

## Patient Rights

**Access:** You have the right to look at or get copies of your protected health information, with limited exceptions. You must make a request in writing to the contact person listed herein to obtain access to your protected health information. You may also request access by sending us a letter to the address at the end of this notice. If you request copies, we will charge you **25¢** for each page, **\$15.00** per hour for staff time to locate and copy your protected health information, and postage if you want the copies mailed to you. If the Practice keeps your health information in electronic form, you may request that we send it to you

or another party in electronic form. If you prefer, we will prepare a summary or an explanation of your protected health information for a fee. Contact us using the information listed at the end of this notice for a full explanation of our fee structure.

**Accounting of Disclosures:** You have the right to receive a list of instances in which we or our business associates disclosed your non-electronic protected health information for purposes other than treatment, payment, health care operations and certain other activities during the past six (6) years. For disclosures of electronic health information, our duty to provide an accounting only covers disclosures after January 1, 2011 [January 1, 2014] and only applies to disclosures for the three (3) years preceding your request. We will provide you with the date on which we made the disclosure, the name of the person or entity to whom we disclosed your protected health information, a description of the protected health information we disclosed, the reason for the disclosure, and certain other information. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests. Contact us using the information listed at the end of this notice for a full explanation of our fee structure.

**Restriction Requests:** You have the right to request that we place additional restrictions on our use or disclosure of your protected health information. Except as noted herein, we are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency). We are required to accept and follow requests for restrictions of health information to insurance companies if you have paid out-of-pocket and in full for the item or service we provide to you. Any agreement we may make to a request for additional restrictions must be in writing signed by a person authorized to make such an agreement on our behalf. We will not be bound unless our agreement is so memorialized in writing.

**Confidential Communication:** You have the right to request that we communicate with you in confidence about your protected health information by alternative means or to an alternative location. You must make your request in writing. We must accommodate your request if it is reasonable, specifies the alternative means or location, and continues to permit us to bill and collect payment from you.

**Amendment:** You have the right to request that we amend your protected health information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or for certain other reasons. If we deny your

request, we will provide you a written explanation. You may respond with a statement of disagreement to be appended to the information you wanted amended. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people or entities you name, of the amendment and to include the changes in any future disclosures of that information.

**Electronic Notice:** If you receive this notice on our website or by electronic mail (e-mail), you are

entitled to receive this notice in written form. Please contact us using the information listed at the end of this notice to obtain this notice in written form.

**Notice of Unauthorized Disclosures:** If the Practice causes or allows your health information to be disclosed to an unauthorized person, the Practice will notify you of this and help you mitigate the effects.

---

## Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the information below.

If you believe that we may have violated your privacy rights, or you disagree with a decision we made about access to your protected health information or in response to a request you made, you may complain to us using the contact information below. You also may submit a written complaint to the U.S.

Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your protected health information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Name of Contact Person: JOHN BRANDEISKY, DPM, FACFAS

Telephone: 732-308-1090

Address: 4249 US 9 NORTH FREEHOLD NJ 07728