Bruce P. Robinson, M.D., F.A.A.D.

Kate E. Lowenthal, M.D., F.A.A.D.

Diplomate American Board of Dermatology

121 East 60th Street, Second Floor

New York, New York 10022

www.BruceRobinsonMD.com

212-750-71212

A. **Introduction**

This HIPAA Privacy Policy contains our Practice policies, procedures, and standards of conduct designed to ensure our compliance with applicable Federal laws and regulations. Failure to abide by the rules, policies and procedures established by this Policy or behavior in violation of any HIPAA law, regulation or rule may result in disciplinary action. Willful failure by any employee of the Practice to comply with the policies and procedures contained in this Plan, will
result in employment dismissal. Consult the Personnel Policy Manual or contact our HIPAA Compliance Personnel if you have any questions about the commitment of our Practice to effective compliance routines.

B. **Compliance Mission Statement**

This Practice strives at all times to maintain the highest degree of integrity in its interactions with patients and the delivery of quality health care. The Practice and its employees will at all times strive to maintain compliance with all laws, rules, regulations and requirements affecting the practice of medicine and the handling of patient information. The protection of the privacy of an individual's health information and the security of an individual's electronic protected health information ("ePHI") is a critical concern to this Practice, and to the trust our patients offer in our treatment of their medical issues.

C. **Privacy Policies**

1. Notice of Privacy Practices

The HIPAA Privacy Regulations require health care providers to furnish patients with a written notice of the Practice's policies and procedures regarding the use and disclosure of protected health information. This Notice of Privacy Practices is the starting point under HIPAA. It describes how the Practice will be handling confidential
patient information in accordance with the HIPAA regulations. Please review it carefully so that you can explain it to patients if asked.

Front desk personnel should provide each patient (new or established), at the time of the first office visit, with a copy of the Notice for review. It should be returned to the front desk prior to the patient being seen by the doctor. The Practice will also keep on hand paper copies of the Notice for patients who ask for a take-home copy. A current copy of the Notice need only be provided once to the patient.

If the Notice is ever materially changed in terms of the description of permitted disclosures, patient rights, the Practice's legal duties, or other privacy practices, then the Notice must again be distributed to each patient.

When the patient receives the Notice, or arrives at the office for a visit after the Notice has been changed, front desk personnel should provide the patient with the Written Acknowledgement form included as Exhibit P4 to this Manual, and ask the patient to sign. This form merely signifies that the patient has received a copy of the Notice.

2. Staff Access to Information

HIPAA provides that staff member job functions should be reviewed to determine the level of PHI access that the staff member strictly needs to do their job. Staff members

should only have the minimum access necessary, and no more.

3. Authorizations

"Authorizations" are basically patient consent forms that contain certain specific provisions required by HIPAA. Typical situations where authorizations are needed are:

- Release of medical records to qualify for life insurance coverage;
- Release of school physical results to the school, for purposes of qualifying for team sports, etc., unless the disclosure involves only immunizations and the parent or guardian has indicated their consent to the release through some other written agreement or through oral assent which has been documented. (You can also simply give the PHI directly to the parent/guardian or patient and direct them to give the information to the school);
- Clinical trial participation (release of information to pharmaceutical company is not for treatment; it's for research, which is not a HIPAA exception);
- Completion of Family Medical Leave Act forms for employers (release of information to employer is not "treatment" – easiest course again is to give the patient the information, and instruct them to give the information to the employer); or
- Psychotherapy notes in the chart (psychotherapy notes are notes by a mental health professional regarding the contents of counseling conversations and do not include such items as medication information, results of clinical tests, summary of diagnosis or symptoms or prognosis or progress to date).

When you fill out the Authorization Form, note the required "expiration date" or "expiration event." This may be any date or event desired by the patient relating to him or her or the purpose of the disclosure. For instance, for authorization to provide the patient's employer with reports for Family and Medical Leave Act purposes, you could specify the expiration date as "termination of employment." For research disclosures only, "none" may be specified as the expiration.

Sometimes you may receive an Authorization form signed by the patient that is on "somebody else's form." For instance, frequently life insurance companies have their medical technicians obtain the patient's signature on a form at the time when all the other paperwork is filled out and the patient gives a blood sample. The life insurance company then sends the form to you, asking for the medical records. Can you accept this form, or do you need to have the patient execute the Practice's own authorization form?

You may accept an outside party's Authorization form provided it has all the elements required by HIPAA. These are:

a. A specific description of information to be used or disclosed;
b. The identification of specific individuals authorized to make the requested use or disclosure of the information;
c. The identification of specific individuals to whom the practice may make the requested use or disclosure of the information;
d. A description of each purpose of the requested use or disclosure;
e. The expiration date of the use or disclosure;
f. A statement of the patient's right to revoke the Authorization at any time in writing along with the procedure for revocation;
g. A statement that the provider may not withhold treatment if the patient refuses to sign the authorization (except as noted below for research, school physicals and other situations where treatment would not normally be provided unless the patient authorized disclosure of his or her PHI);
h. A statement that the PHI used or disclosed may be subject to re-disclosure by the party receiving the information and may no longer be protected;
i. Patient's signature and date.

If the form you are sent does not have these elements, have the patient execute the Practice's Authorization Form. Please be sure to give the patient a copy of the authorization, when it is signed, for their records. This is required by HIPAA.

4. Minors and Incompetent Patients

As noted, minors and incompetent patients generally cannot sign the Written Acknowledgment form for themselves. Typically, they do not have the legal authority to do this. Only the person(s) who have the ability to give informed consent for the minor or incompetent patient, under state law, can exercise these rights.

Normally, in the case of a minor, it is the parent who has such right to give informed consent for the child. Therefore it is the parent who signs the Written Acknowledgment or the Authorization or other forms and who exercises the child's HIPAA rights as a patient.

Exceptions to this policy may occur depending upon state law and are noted here.

5. Friends and Family

"Friends and family" pose a special challenge. These are the people who come with the patient to the doctor's office, or who pick up the phone when you call the patient's home.

Under HIPAA, friends and family, even spouses, are not entitled to the patient's PHI. Only the patient himself or herself has an absolute right to the PHI. The exception is parents of minor children or other legal guardians, who are generally to be treated for HIPAA purposes as if they were the patient, as noted above.

Having said this, HIPAA does permit some sharing of information with friends and family. HIPAA specifies that the Practice may, without written Authorization, disclose to a "family member, other relative, or a close personal friend of the [patient], or any other person identified by the [patient], the PHI directly relevant to such person's involvement with the [patient]'s care or payment related to the [patient's care]."

However, there are some "strings attached." To disclose to these people (referred to in this Manual as "friends and family"), one of the following must apply:

- the Practice obtained the patient's oral or written agreement to disclosing information to the person in question;
- the Practice provided the patient with the opportunity to object to the disclosure, and the patient did not object;
- the Practice could "reasonably infer from the circumstances, based on the exercise of professional judgment, that the [patient] does not object to the disclosure," such as when the friend or family member accompanies the patient into the exam room, or when a child arrives at the doctor's office in the care of a babysitter (presumably the parent wants the babysitter to receive all resulting diagnoses and care instructions), or where a patient arrives from the nursing home in the care of a nurse's aide;
- it is an emergency situation or the patient is incapacitated, so that there is no chance to provide the patient with the opportunity to agree or object;
- the friend or family member has been sent to pick up filled prescriptions, medical supplies, x-rays, or other PHI, in which case the practice is permitted to make a reasonable inference as to the patient's best interest, in accordance with common medical practice.

If a patient wishes to identify a family member or other person with whom their medical information may be shared, the patient should be given the opportunity to designate individuals to whom it is acceptable to make a disclosure of PHI. This determination should be kept inside the patient's chart and updated as designated acceptable PHI recipients are added or dropped. It is not necessary that the patient indicate this in writing, including adding or dropping individuals from the list, since oral agreement suffices. Also, the friends

and family who are named by the patient do not represent the only individuals authorized to receive the patient's PHI. As noted, there may be situations where the Practice is entitled to infer that the patient does not object to the release of information, such as in the case when the friend or family member accompanies the patient into the exam room, or a child arrives at the doctor's office in the care of a babysitter.

Simple appointment reminders can generally be left with family members even if the family member is not explicitly designated as a PHI recipient by the patient. However, check the patient's file to see if the patient has requested an alternative means of communication, and if so, honor it. In any event, do not indicate to the family member the reason for the patient's doctor visit.

6. Patient Access to Chart

Except for psychotherapy notes, patients generally have the right to inspect and obtain a copy of their medical chart. Have the patient fill out the Practice's "Request for Access to Medical Information" form. Generally, the Practice has 30 days to comply with a request for access, or 60 days if the information requested is not on-site.

The Practice must honor the patient's request to have the information delivered in a particular format, if this can be easily done. The Practice may be entitled to demand a copying charge.

If the patient merely wants to look at the file, not copy it, arrange a mutually convenient time and place for this to be done.

The patient's request for his or her PHI may be denied in very limited circumstances only. Access may be denied if:

- the file contains information obtained from a source other than a health care provider under a promise of confidentiality, and the access would reveal the source;
- the information requested has been compiled in a research trial that is still underway, and the patient previously agreed in writing that access would not be allowed until the study was completed;
- a licensed health care professional has made a judgment that access would likely endanger the life or physical safety of the patient or someone else;
- the file makes reference to another person, and the licensed health professional makes a judgment that access would likely result in substantial harm to that other person;
- the information is requested by the patient's personal representative and the licensed health professional makes a judgment that access would likely result in substantial harm to the patient or another person.

If access is denied, the patient has a right to review the decision to deny access, unless it is for either of the first two reasons noted above. This review must be done by a licensed health care professional who was not involved in the original decision to deny access. Be sure to document any denials.

7. Patient Amendment of Chart

The patient has a right to request an amendment to their medical record (so long as the Practice maintains it) if he or she believes it is incorrect or incomplete. To request an amendment, the patient should complete the Practice's form "Request to Amend Medical Information". The amendment must be dated and signed by the patient.

The Practice may deny the patient's request for an amendment if it is not in writing or does not include a reason to support the request. In addition, the Practice may deny a request to amend information that:

j. was not created by the Practice, unless the person or entity that created the information is no longer available to make the amendment;

k. is not part of the medical information kept by or for the Practice;

l. is not part of the information which the patient would be permitted to

inspect and copy; or

m. is accurate and complete.

The Practice must respond to the request to amend within 60 days.

8. Incidental or Inadvertent Disclosures

Taken literally, HIPAA's prohibition against the disclosure of PHI would probably bring most medical practices to a standstill. For instance, the mere announcement of a patient's name in the waiting room is a disclosure of PHI – the patient's name. The same applies to sign-in sheets, overheard conversations with the check-in or check-out clerk regarding follow-up appointments, or other common situations where one patient inadvertently learns information about another patient.

Overheard conversations and other such inadvertent disclosures are called "incidental disclosures." Under HIPAA, incidental disclosures are not violations, provided that the Practice has taken reasonable steps to "safeguard" PHI and avoid incidental disclosures to the extent possible.

9. Faxes, Answering Machines, Messages, Email

As noted, HIPAA requires "reasonable safeguards" to avoid the disclosure of PHI. Although some inadvertent disclosures will be excused as "incidental," the Practice has established the following procedures to minimize the likelihood of HIPAA violations:

- Faxing is less secure than mailing. It could be faxed to the wrong number or it may be seen by an unintended person upon arrival at the destination. If practical, mail rather than fax.
- If you fax information, be sure to double-check the fax number to minimize the chances of a fax going to the wrong number; if you have any doubts regarding the number, call the intended recipient to confirm the fax number. Ideally, you should also follow-up with the intended receipient to ensure the fax was received.
- Faxes to hospitals, other physicians, labs, and other routine recipients are acceptable However, double check the fax number before sending, and always use a cover sheet indicating that PHI may be attached and that if the fax has gone to the wrong person, it should be returned or destroyed.
- Leaving messages on answering machines for appointment reminders is acceptable. Do not indicate the reason for the visit. Do not leave messages regarding lab or diagnostic results (even negative results) or any kind of medical information on the answering machine. Just ask that the call be returned. Do not leave a message of any kind on the answering machine if the answering machine tape does not furnish some reasonable indication that you have reached the correct number.
- Leaving messages with family members at home is also acceptable for appointment reminders. Indicate only that an appointment is scheduled, not what the visit is for. Do not leave any other kind of information, unless the Practice's records show that the person on the phone is a "friend or family" designated by the patient to be a permitted recipient of PHI.
- Leaving messages at work is very sensitive. Avoid calling the work number, but if necessary ask for a return call and nothing more.
- Appointment reminders by postcard is acceptable, so long as the appointment is of a routine nature.
- Do not use email to communicate with patients unless the Privacy Officer has developed a specific written policy to control the use of this form of communication.
- Do not share passwords for email, EHR software or other electronic sources PHI with other staff.
- Staff are expected to log off their individual workstation at the end of the day or at any time they are away from their workstation for a prolonged period of time.