

HIPAA Policy & Procedures Manual

Bruce S. Dobozi, M.D.

Allergy & Asthma

121 East 60th Street

New York NY 10022

EXPLANATION AND GUIDE

Form: Practice HIPAA Policies and Procedures Manual

Purpose: The Final Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) is effective on April 14, 2003. Two main components of the Final Privacy Rule are 1) to have policies and procedures in place to protect the privacy of the personal health information your practice handles; and 2) to provide certain rights to patients with respect to the uses and disclosures of their personal health information as defined under the Final Privacy Rule. This manual contains the following policies and procedures as well as model forms where applicable:

- Policy: 1 Confidential Patient Communications
- Policy: 2 Inspect and Copy Medical Records
- Policy: 3 Amend Medical Records
- Policy: 4 Restrict Uses and Disclosures
- Policy: 5 Accounting of Uses and Disclosures
- Policy: 6 Minimum Necessary (De-Identification of PHI)
- Policy: 7 Notice of Privacy Practices
- Policy: 8 Staff Facsimile
- Policy: 9 Staff E-mail
- Policy: 10 Appropriate Safeguards
- Policy: 11 Business Associates
- Policy: 12 Training
- Policy: 13 Privacy Violations
- Policy: 14 Patient Complaint Process for Privacy Concerns

Each policy, procedure and model form has been reviewed by our Privacy Officer and/or Privacy Committee and customized for our practice.

State law must also be recognized in our policies and procedures (e.g., NY State law defines specific charges allowed for copying, or specific timeframes are defined for responding to requests from an individuals for certain information). If NY State law is more stringent than the Final Privacy Rule, the Final Privacy Rule requires that state law must be followed.

The implementation specifications of the HIPAA Privacy Rule require our medical practice to develop and implement policies and procedures appropriate for our practice, reflecting the practice's business practices and workforce.

We will continue to add policies and procedures to your privacy manual as necessary to reflect your compliance efforts.

Table of Contents

Policy: 1	Confidential Patient Communications	Page 4
Policy: 2	Inspect and Copy Medical Records	Page 6
Policy: 3	Amend Medical Records	Page 11
Policy: 4	Restrict Uses and Disclosures	Page 15
Policy: 5	Accounting of Uses and Disclosures	Page 18
Policy: 6	Minimum Necessary (De-Identification of PHI)	Page 23
Policy: 7	Notice of Privacy Practices	Page 26
Policy: 8	Staff Facsimile	Page 38
Policy: 9	Staff E-mail	Page 41
Policy: 10	Appropriate Safeguards	Page 47
Policy: 11	Business Associates	Page 49
Policy: 12	Training	Page 63
Policy: 13	Privacy Violations	Page 66
Policy: 14	Patient Complaint Process for Privacy Concerns	Page 69

Subject: Confidential Patient Communications

Policy: 1

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 1 (including Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to provide individuals with the right to receive confidential communications of their personal health information by alternate means other than those traditionally provided by the practice.

Procedures:

1. Process. *Dr. Dobozi* will receive and process all inquiries regarding an individual's request to receive communications regarding their personal health information confidentially (e.g., the practice will not call the individual's home, only their cell phone).
2. Content of Request to Receive Information Confidentially Form. Upon request from an individual to receive information relating to their treatment confidentially, *Dr. Dobozi* will provide the individual with the *Request to Receive Information Confidentially* form (See Attachment A). The following information must be included to process the request:
 - a. Name and address
 - b. Very specific information as to how or where the individual wishes the practice to communicate with him/her.
 - c. The reason for the request does not need to be disclosed.
3. Accommodation of Request. The practice will attempt to accommodate all **reasonable** requests.
 - a. Staff will complete the form indicating whether the request is granted or denied.
 - b. If the request is denied, a reason must be provided.
 - c. If a request to receive information confidentially is granted, the practice must adhere to this request unless an alternate means of communication is requested in writing.
 - d. Failure to adhere to a request granted by the practice may subject staff member to disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.
4. A completed request form must be filed in the individual's medical record and a copy provided to the individual.

ATTACHMENT A

REQUEST TO RECEIVE INFORMATION CONFIDENTIALLY

You have the right to receive confidential communications of your personal health information by alternate means or at alternate locations. **Please be aware that you are not required to provide a reason for your request.** *The practice will attempt to accommodate all **reasonable** requests.*

Patient Name:	Social Security/MRN:
Date of Birth:	Phone Number:
Street Address:	City, State, Zip Code:

Please be very specific as to where or how you wish the practice to communicate with you:

Patient/Guardian Signature: _____ Date: _____

*Internal use only:
Request:*

- Granted
- Denied

If denied, reason:

Completed By: _____ Date of Completion: _____

Subject: Inspect and Copy Medical Records

Policy: 2

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (including Attachments A and B)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to provide individuals with the opportunity to inspect the medical record that has been created by this practice to treat the individual and is used to make decisions about their care.

Procedures:

1. Process. *Dr. Dobozi* will receive and process all requests to inspect and copy medical records. This includes medical and billing records.
 - a. Records related to an individual's care may be disclosed to an authorized person such as a parent or guardian upon proper proof of a legitimate legal relationship.
2. Upon request from an individual to inspect and copy medical records, staff will provide the individual with a *Request to Inspect and Copy Medical Records* form (See Attachment A). The individual must use this form to submit his/her request in writing to the practice.
3. The Privacy Officer will consult with physicians to determine whether any reasons exist to restrict or deny an individual or his/her representative access to requested portions of the medical record.
4. Right to Deny a Request. A request to inspect and copy medical records may be denied for the following reasons:
 - a. The practice does not possess the information requested. (Provide location of information if known)
 - b. The individual requests psychotherapy notes and the Privacy Rule provides our practice with the discretion to deny requests to inspect and obtain a copy psychotherapy notes.
 - c. The information requested was obtained from a third party under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of information.
 - d. The information requested has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding therefore the practice is not required to grant your request.
 - e. The information requested is subject to or exempted by the Clinical Laboratory Improvements Amendments (CLIA) of 1988.
 - f. The information requested was/is being created or obtained in the course of on-going research that includes treatment and you agreed to the denial of access as a condition of participation in the program. Your right of access will be granted when the program is complete.

- g. The information requested is contained in records subject to the federal Privacy Act, 5 U.S.C. §552a, which protects personal information about individuals held by the federal government, and this denial meets the requirements of that law.
5. Right to Appeal a Request. If access to requested information has been denied *for any of the following three reasons listed below*, an individual has the right to have the denial reviewed by another licensed healthcare professional in the practice who did not participate in this denial. The individual must submit a written request to the Privacy Officer and will receive a written response within a reasonable period of time.
 - a. A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger the individual's life or physical safety or the life or physical safety of another person.
 - b. The information requested makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.
 - c. The individual is the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to the individual.
6. Complaint to Secretary of HHS. An individual may file a complaint regarding a denial with the Secretary of the U.S. Department of Health and Human Services. Complaints must be in writing, provide the name of the practice, a description of circumstances leading to the acts believed to violate the Privacy Rule, and be filed within 180 days of the alleged violation.
7. Privacy Officer will make a determination within seven (7) business days whether to grant or deny a request to inspect and/or copy requested portions of the medical record.
8. Record Inspection. The receptionist in the office will schedule a mutually agreeable time with individual to allow inspection of the medical record. Inspection will take place only on practice premises.
9. Copy of Record. If the individual would like to copy his/her records, the practice may charge reasonable fees for the cost of copying records, mail or other minimal costs associated with the request. The individual must complete the remainder of the *Request to Inspect and Copy Medical Records* form if they wish to receive copies of specific portions of the medical record (Attachment A).
10. Content of Copied Records. The receptionist or Privacy Officer will copy only those materials requested by the individual and release the medical record as specified by the individual.
11. Completed Request Form. The receptionist or Privacy Officer will complete the bottom portion of the *Request to Inspect and Copy Medical Records* form indicated *For Internal Use Only* upon delivery to individual. If a request is denied, a letter will be mailed via certified U.S. mail indicating the reason for the denial (See Attachment B).
12. Filing of Request. A completed request form must be filed in the individual's medical record for up to six years and a copy provided to the individual.

**ATTACHEMENT A
REQUEST TO INSPECT AND COPY MEDICAL RECORDS**

Patient Name:	Social Security/MRN:
Date of Birth:	Phone Number:
Street Address:	City, State, Zip Code:

Please specify what records you would like to inspect:

- All records
- All records between the dates of _____ and _____.
- Records pertaining to _____

Please specify what records you would like to copy:

- All records
- All records between the dates of _____ and _____.
- Records pertaining to _____

Please specify method of release:

- Pick-up
- Certified Mail to:

*** Please note: I understand that a reasonable fee will be charged in the amount of \$_____ for this service including the cost of copying records and mailing.**

Name:	Title/Business:
Street Address:	City, State, Zip Code:
Phone Number:	Relationship to Patient:

Patient/Guardian Signature: _____ Date: _____

Internal use only:

Completed By: _____

Date Records Mailed/Picked-up: _____

Fees for Copying and Mail: _____

ATTACHMENT B

PATIENT DENIAL LETTER

Bruce S. Dobozi, M.D. Allergy & Asthma

121 East 60th St, New York, NY 10022

Phone: 212-826-0815/Fax: 212-826-0819/Email: bdobozi@earthlink.net

Date
Name
Address
City, State Zip

Dear:

In accordance with the Final Rule for the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), our practice is unable to grant your request to inspect and obtain a copy of the information you requested in your medical record for the following reasons (s):

_____ The practice does not possess the information requested. (*Provide location of information if known*):_____.

_____ You have requested psychotherapy notes and the Privacy Rule provides our practice with the discretion to deny requests to inspect and obtain a copy psychotherapy notes.

_____ The information you have requested was obtained from a third party under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of information.

_____ The information you have requested has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding therefore the practice is not required to grant your request.

_____ The information you have requested is subject to or exempted by the Clinical Laboratory Improvements Amendments (CLIA) of 1988.

_____ The information you have requested was/is being created or obtained in the course of on-going research that includes treatment and you agreed to the denial of access as a condition of participation in the program. Your right of access will be granted when the program is complete.

_____ The information you have requested is contained in records subject to the federal Privacy Act, 5 U.S.C. §552a, which protects personal information about individuals held by the federal government, and this denial meets the requirements of that law.

If access to requested information has been denied *for any of the following three reasons listed below*, you have the right to have the denial reviewed by another licensed healthcare professional in the

practice who did not participate in this denial. If you choose to have this denial reviewed, please submit a written request to our Privacy Officer, Bruce S. Dobozi, M.D.. You will receive a written response within a reasonable period of time. You may file a complaint regarding this denial with the Secretary of the U.S. Department of Health and Human Services. Complaints must be in writing, provide the name of the practice, a description of circumstances leading to the acts believed to violate the Privacy Rule, and be filed within 180 days of the alleged violation.

_____ A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger your life or physical safety or the life or physical safety of another person.

_____ The information you have requested makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.

_____ You are the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to you.

Please do not hesitate to contact our Privacy Officer if you have any questions regarding this letter.

Sincerely,

Bruce S. Dobozi, M.D.
Physician

Subject: Amend Medical Records

Policy: 3

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (including Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to provide individuals with the right to request an amendment or clarification of information in his/her medical record if the individual believes the information is inaccurate or incomplete.

Procedures:

1. Process. The receptionist or Privacy Officer will receive and process all requests to amend medical records.
2. Content of Request. Upon request from an individual to amend his/her medical record, staff will provide the individual with the *Request to Amend Medical Records* form (See Attachment A). A request to make an amendment must include the following and **may be refused if the following elements are not met:**
 - a. Individual must submit the request in writing to the receptionist or Privacy Officer.
 - b. Individual must describe what he/she would like the amendment to say and reasoning for why the change should be made. Examples of the types of entries to be amended may include:
 - i. Visit notes
 - ii. Nurse notes
 - iii. Prescription information
 - iv. Patient history
 - c. The request for amendment must be dated, signed by individual
 - d. The request for amendment must also be notarized
3. Basis to Deny Request. A request to amend information may be refused under the following circumstances:
 - a. The information is not part of the medical information kept by the practice
 - b. The practice believes the information the individual provided to the practice is inaccurate or incomplete.
 - c. Information created by third parties may not be changed.
 - d. The information is not available for inspection in accordance with the law
 - e. The information is accurate and complete.
 - i. The Privacy Officer will bring all questions regarding accuracy to the treating physician.
 - f. Comments must be provided on the *Request to Amend Medical Records* form to identify the basis of the denial.

4. Timing of Response. The Privacy Officer will respond to the request for an amendment no later than sixty (60) days after receipt of the request.
5. Granted Requests. If a request is granted in whole or in part, the Privacy Officer must:
 - a. Change the information in the record
 - b. Complete the bottom portion of the form indicated for *Internal Use Only* and inform the individual of the change by providing him/her with a completed request form
 - c. Notify other individuals if protected health information is incorrect.
6. Completed Request Form. A completed request form must be filed in the individual's medical record for up to six years.

ATTACHMENT A

REQUEST TO AMEND MEDICAL RECORDS

If you believe there is information in your medical record that may be inaccurate or incomplete, you have the right to request an amendment or clarification of information in your record.

Patient Name:	Social Security/MRN:
Date of Birth:	Phone Number:
Street Address:	City, State, Zip Code:

Please specify the exact amendment you would like to make to your medical record:

Please describe your reasoning for the above requested amendment:

**If additional space is required, please attach a separate, typed or neatly written statement to this request form.*

Patient/Guardian Signature: _____ Date: _____

Notary Public: _____

Internal use only:

Date request received: _____

Request:

- Granted
- Denied
- Granted in part/Denied in Part

If denied in whole or in part, reason for denial:

- Information was not created by this practice
- Information is not part of the medical information kept by this practice
- Information provided by the requesting party is inaccurate or incomplete
- Information in the record is accurate and complete
- Information is not available for inspection in accordance with the law

Comments:

Completed By: _____ Date of Completed Amendment: _____

Title: _____

Please Note: If your request has been denied, in whole or in part, you have the right to submit a written statement disagreeing with the denial to the practice. Please submit your statement to (*Bruce S. Dobozi M.D., Privacy Officer, 121 East 60th St NY, NY 10022*). If you do not provide us with a statement of disagreement, you may request that we provide to you copies of your original request for amendment, our denial, and any disclosures of the protected health information that is the subject of the requested amendment. Additionally, you may file a complaint with our Privacy Officer or the Secretary of the U.S. Department of Health and Human Services.

Subject: Restrict Uses and Disclosures

Policy: 4

Initial Date: December 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (including Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**’s policy to provide individuals with the right to request restrictions on how the practice makes certain uses and disclosures of protected health information for treatment, payment or healthcare operations.

Procedures:

Definition:

1. Protected Health Information (PHI). The final rule defines PHI as individually identifiable health information that is transmitted by electronic media; maintained in any electronic medium such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium (i.e. paper, voice, Internet, fax etc.).
2. Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from an individual and that is created or received by a health care provider 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, and which identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
3. Process. The receptionist or Privacy Officer will receive and process all requests to restrict how the practice makes certain uses and disclosures of protected health information for treatment, payment and healthcare operations. The practice is not required to agree to a request but if it does, it must document and strictly abide by the restrictions.
4. Upon receipt of a request to restrict uses and disclosures from an individual, staff will provide the individual with the *Request to Restrict Uses and Disclosures* form (See Attachment A).
5. Content of Request. Each individual request must be in writing and include the following:
 - a. What information the individual would like to limit
 - b. Whether the individual wants to limit our use, or disclosure or both
 - c. To whom the individual want the limits to apply (e.g., disclosures to parents, children, spouse, etc.) See Attachment A.

6. Compliance with Request. The practice is not required to agree to an individual's request or it may not be able to comply with the request. However, the practice should do all that it can to accommodate the request. Examples of requests may include:
 - a. Restriction on how much information the practice provides to family members regarding the individual's treatment or payment for care.
 - b. Restrictions on certain types of marketing materials related to his or her care or treatment.
 - c. Restrictions or limitations on disclosures of certain types of information including but not limited to:
 - i. Phone number
 - ii. Spouses name
 - iii. Occupation
7. Discuss Request with Individual. If an individual requests a restriction that is not in their best interests or may impede the delivery of care to the individual, the Privacy Officer will discuss the request with the individual prior to granting or denying the request.
8. Basis for Noncompliance with Request. The practice may not be able to comply with a request to restrict uses and disclosures by an individual for the following reasons:
 - a. The practice cannot in good faith manage the request
 - b. The request is unreasonable
 - c. The information is required to provide emergency treatment to the individual
9. The Privacy Officer will complete the bottom portion of the form indicated for *Internal Use Only* and notify the individual whether the request is accepted or denied by providing the individual with a copy of the request.
10. Completed Request Form. A completed request form must be filed in a visible area within the individual's medical record to enable compliance with the request.
11. Termination of Restriction. If the practice and the party originally requesting a restriction agree to the termination of a restriction, the practice must obtain agreement in writing documenting specifically the information no longer subject to restriction and identifying information that may be subject to restriction even after termination.
12. Compliance. Employees have a duty to comply with the policies and procedures set forth by the practice. Any employees found to violate the practices' policies and procedures are subject to disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.

**APPENDIX A
REQUEST TO RESTRICT USES AND DISCLOSURES**

You have the right to request restrictions on how this practice makes certain uses and disclosures of your personal health information for treatment, payment and healthcare operations. **Please note that this practice is not required to grant your request, but we will do our best to accommodate your wishes.** If this request is approved, it shall not apply if the information for which you request to limit is required to provide emergency treatment to you.

Patient Name:	Social Security/MRN:
Date of Birth:	Phone Number:
Street Address:	City, State, Zip Code:

Please describe in detail the type of information you would like to limit:

Please specify whether you would like to limit the following:

- Practice Use of the above specified information
- Practice Disclosure of the above specified information
- Both the Use and Disclosure of the above specified information

To whom would you like these limits to apply?

- Parent(s)
- Spouse
- Children
- Guardian
- Other

Describe: _____

Patient/Guardian Signature: _____ Date: _____

Internal use only:

Request:

Granted

Denied

Reason for Denial:

Completed By: _____ Date: _____

Subject: Accounting of Uses and Disclosures

Policy: 5

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 3 (including Attachments A and B)

Approved: Bruce S. Dobozi, M.D. Date: April 1, 2003

P. R. Physician, M.D. Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to provide individuals with the right to receive an accounting of the disclosures of their protected health information made by the practice and its business associates.

Procedures:

Definitions

1. Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from an individual and that is created or received by a health care provider 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, and which identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
2. Protected Health Information (PHI). The final rule defines PHI as individually identifiable health information that is transmitted by electronic media; maintained in any electronic medium such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium (i.e. paper, voice, Internet, fax etc.).
3. Designated Record Set. A group of records maintained by or for the practice that is:
 - a. The medical records and billing records about individuals maintained by or for the practice
 - b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan
 - c. Used, in whole or in part, by or for the practice to make decisions about the individual.
4. Right to an accounting of Uses and Disclosures of PHI. Individuals have the right to receive an accounting of the disclosures of their protected health information that is maintained by the practice and its business associates. All requests must be submitted in writing and submitted to the reception desk for appropriate processing.

- a. All requests must be for disclosures dated **AFTER April 14, 2003**.
 - b. All requests must state a time period **not longer than six (6) years back**.
5. Disclosures exempt from the accounting rule. The practice is not required to grant a request for an accounting if the disclosure was made for the following purposes:
- a. Required to carry out treatment, payment, and healthcare operations as provided in §164.506 of the Final Privacy Rule
 - b. The disclosure is made to the individual about himself or herself
 - c. For national security or intelligence purposes (§164.512(k)(2))
 - d. Provided to law enforcement officials or correctional institutions (§164.521(k))
 - e. Authorized disclosures by the individual (§164.508)
 - f. Incidental uses or disclosures otherwise permitted or required as provided for in §164.502
 - g. The use or disclosure occurred prior to the April 14, 2003 Final Privacy Rule compliance date
 - h. Permitted disclosures to business associates as provided for in §164.512
6. Content of Written Accounting. The disclosure to the individual must include:
- a. The date of each disclosure
 - b. Name and address of each recipient of the information
 - c. A brief description of the information disclosed
 - d. The purpose for which the information was disclosed
 - e. Copies of all requests for disclosure
7. Multiple Disclosures For Same Purpose. If the practice makes multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may provide:
- a. The information listed in paragraph 6 for the first disclosure
 - b. The frequency, periodicity, or number of disclosures made
 - c. The date of the last such disclosure during the accounting period.
8. Requests in Writing. Upon receipt of a request for an accounting from an individual, staff will provide the individual with the *Request for an Accounting of Uses and Disclosures* form (See Attachment A). The request will be submitted to the receptionist or Privacy Officer for a prompt evaluation and response.
- a. The individual must state whether he/she would like the accounting in electronic or paper form.
 - b. One request in a twelve-month period will be provided to an individual at no charge.
 - c. The practice will charge a reasonable fee for all additional requests within a twelve-month period.
 - d. **Staff must notify the individual as to the cost of fulfilling his/her additional request and provide the individual with the opportunity to withdraw or modify his/her request in order to reduce the fees before fees are due (See Attachment A).**

9. Response time for request. The Privacy Officer will respond to an individual's request in fewer than thirty (30) days after receipt of the request for an accounting and either provide the accounting or provide a written statement that there will be a delay, the reasons for the delay, and the date by which the information will be provided.
10. Time extension to fulfill request. A single extension of no more than thirty (30) days is available to the practice if the individual is notified of the delay, in writing, within the original thirty (30) day time limit. The Privacy Officer is responsible for all extension requests made by the practice.
11. Documentation of Release of Accounting Information. The practice must maintain a record of the release of disclosure accounting information for a period of six years from the date of the release.
 - a. The Privacy Officer will document all requests for information on the *Log to Track Disclosures of Protected Health Information* form (See Attachment B).
 - b. The record of release of the accounting information must be kept in the individual's medical record.

**ATTACHMENT A
REQUEST FOR AN ACCOUNTING OF USES AND DISCLOSURES**

You have the right to request an accounting of uses and disclosures of your protected health information. This accounting does not include uses and disclosures related to treatment, payment, healthcare operations, disclosures for which you may have already provided written authorization, national security intelligence or uses and disclosures made to correctional institutes or law enforcement officials. One accounting per year shall be provided at no charge. Additional requests for accountings in the same calendar year shall be subject to additional fees.

Patient Name:	Social Security/MRN:
Date of Birth:	Phone Number:
Street Address:	City, State, Zip Code:

*Please specify the dates for which you would like an accounting: **Please note: All requests must be for disclosures after April 14, 2003 and cannot be for a period of more than six (6) years prior to the date of your request for an accounting.***

Accounting between the dates of _____ and _____.

Format of your accounting:

Paper Electronic

Please specify method of release:

Pick-up Certified Mail to:

*** Please note: A reasonable fee will be charged for the cost mailing**

Name:	Title/Business:
Street Address:	City, State, Zip Code:
Phone Number:	Relationship to Patient:

Patient/Guardian Signature: _____ Date: _____

Internal use only:

Completed By: _____ Date: _____

ATTACHMENT B

Log to Track Disclosures of Protected Health Information

Patient Name _____

The Final Privacy Rule requires **Bruce S. Dobozi, M.D. [Allergy & Asthma]** to keep a log of all disclosures of PHI for reasons other than treatment, payment, and healthcare operations and those disclosures authorized by the patient, for which you did not receive a signed authorization from the patient. The practice must retain documentation and tracking log for each patient for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. For each disclosure complete the following:

DATE	DESCRIPTION OF DISCLOSURE	DESCRIPTION OF PHI	Who Requested	To Whom PHI Was Disclosed	Approve/Deny (+ Initials)	REASON FOR DENIAL, COMMENTS

Subject: Minimum Necessary

Policy: 6

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 3

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to only disclose the amount of confidential personal health information necessary to achieve the purpose of the request.

Procedures:

All uses, disclosures of, or requests for protected health information (PHI) will be limited to the minimum amount necessary to accomplish the stated purpose. Professional judgment will determine the amount of information to be released. The minimum necessary standard is not intended to impede the provision of quality health care.

Disclosures of personal health information between providers for treatment, payment and health care operations, or pursuant to an authorization without complying with this requirement are exempt from the minimum necessary rule.

Definitions

1. Protected Health Information (PHI). The final rule defines PHI as individually identifiable health information that is transmitted by electronic media; maintained in any electronic medium such as magnetic tape, disc, optical file; or transmitted or maintained in any other form or medium (i.e. paper, voice, Internet, fax etc.).
2. Individually Identifiable Health Information (IIHI). A subset of health information, including demographic information collected from an individual and that is created or received by a health care provider 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, and which identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
3. Access to Medical Records. Access to PHI will be granted only to those staff members who have a need to access such information to fulfill his/her job responsibilities.
 - a. Role based access has not been adopted by this practice which allows only certain people to access certain information For example:

- i. The billing manager may access an individual's contract and billing information but not medical history
 - ii. The treating physician has full access to the individual's medical history and subsequent treatment records.
 - b. The Security Officer will grant access rights to new employees based on their job responsibilities.
 - c. The Security Officer will modify an employee's access rights if his/her job responsibilities change.

- 4. Uses of PHI. Staff members with a need to access PHI to carry out their job function will be identified and receive specific training on the minimum necessary standard.
 - a. Staff members who access PHI as part of their job responsibilities will be taught what specific information they may access as part of their assigned duties.
 - b. The practice will make reasonable efforts to limit the access of its staff to only the information appropriate to their job requirements.
 - c. Staff members should not be reviewing or using other parts of an individual's medical record or another persons records if they do not need to.

- 5. Exceptions to the Minimum Necessary Rule. The minimum necessary standard **DOES NOT** apply to the following:
 - a. Disclosures to or requests by a health care provider for treatment purposes.
 - b. Disclosures to the individual who is the subject of the information.
 - c. Uses or disclosures made pursuant to an individual's authorization.
 - d. Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
 - e. Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
 - f. Uses or disclosures that are required by other law if use or disclosure complies with and is limited to the relevant requirements of such law.

- 6. Routine Disclosures. For routine and recurring disclosures, the rule requires the practice must limit the disclosures to the amount reasonably necessary to achieve the purpose of the disclosures.
 - a. Medical information may be disclosed to other healthcare providers who a patient has consulted with so that continuity of care is ensured.
 - b. Information regarding diagnosis & date of onset of a condition may be released in order to process insurance claims.
 - c. We normally require consent to transfer records to another physician, however we will provide them without your consent if it is deemed to be in your best interest.

- 7. Non Routine Disclosures.
 - a. Typically only a diagnosis & date of onset of a condition would be provided to an insurance company to process a claim. Additional information would require your consent.
 - b. These criteria must be used to review these disclosures on an individual basis.

- 8. Routine, Recurring Requests.

- a. The receptionist or Privacy Officer must identify what information is reasonably necessary for the purpose of the request
 - i. Examples would include a date of onset of asthma to determine issues of pre-existing condition. Information to aid with the care of a child in school will be provided to appropriate school authorities.
 - b. The practice must limit the request for protected health information to that information only.
9. All Other Disclosures. The practice must develop criteria designed to limit the PHI disclosed to the minimum necessary to achieve the purpose of the request.
- a. The practice has a responsibility to verify that uses and disclosures are indeed for treatment purposes and therefore are not subject to the minimum necessary rule.
 - b. In any instance in which the identity or authority of a requestor is not known to the practice, staff must obtain applicable documentation, statements, or representations in support of the purpose of the request and/or identity of the requestor.
10. Practice Requests for PHI. Staff must review each request on an individual basis and must limit any request it makes for PHI to that which is reasonably necessary to accomplish the purpose of the request.
- a. Requests for an entire medical record should only be made when necessary and not if staff can achieve the purpose of the request by limiting the information requested.
11. Training. All staff receives privacy training. Staff whose job responsibilities include the use and disclosure of PHI will be trained to adhere to the minimum necessary requirement.
- a. New staff will not make any uses and disclosures of PHI until training is completed.
 - b. Staff whose job responsibilities change to include access to PHI will not make any uses and disclosures of PHI until training is completed.
12. Compliance Monitoring. To ensure compliance with the minimum necessary requirements the receptionist or Privacy Officer or others will periodically monitor audit trails (*or other if applicable*) and check particularly vulnerable areas (*such as all requests for entire medical record*).
- a. Reviews will be triggered when there are special complaints or incidents.
 - b. This compliance process will result in feedback to staff on areas needing more attention and may necessitate the redesign of work processes or procedures to enhance compliance.
13. Compliance. Employees have a duty to comply with the policies and procedures set forth by the practice. Any employees found to violate the practices' policies and procedures are subject to disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.

Subject: Notice of Privacy Practices

Policy: 7

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (including Attachments A and B)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to provide individuals with a Notice of Privacy Practices prior to an individual's first date of service and to make a good faith effort to obtain written acknowledgment that the Notice was received by the individual.

Procedures:

1. Process. Staff must provide all individuals with a Notice of Privacy Practices and make a good faith effort to obtain written acknowledgement that the Notice was received (See Attachment A). All individuals must receive the Notice after April 14, 2003, the effective date of the Final Privacy Rule.
2. Individuals Who Receive the Notice. All individuals who request treatment from the practice must receive the Notice as well as those individuals who request a copy of the Notice from the practice.
 - a. New patients must receive the Notice prior to their first date of service. The practice may provide the Notice to the individual in the office prior to his/her visit and is not required to send the Notice via mail or facsimile prior to the visit.
 - b. Existing patients must receive the Notice upon their first office visit after the April 14, 2003 compliance deadline.
 - c. The Privacy Officer will be responsible for ensuring that an updated version of the Notice is always present on the practice website.
3. Written Acknowledgment. Staff will take the following steps to obtain written acknowledgement of receipt of the Notice (See cover page of Attachment A):
 - a. Ask the patient to initial the cover page of the Notice and return it to the practice (Attachment A); **Or**
 - b. Ask the patient to initial a separate acknowledgement list (See Attachment B).
 - c. Staff is not required to obtain written acknowledgement of the Notice in emergency situations.
4. Acknowledgment Not Obtained. Staff is not required to obtain a signature from an individual. Patient treatment will not be affected in any manner if an individual fails to provide written acknowledgement of receipt of the Notice. An individual may refuse or

fail to provide their signature documenting they received the Notice. If a signature indicating receipt of the Notice cannot be obtained, staff must:

- a. Document that a good faith effort to obtain such acknowledgement was made;
 - b. The efforts taken to obtain the written acknowledgement of receipt of the Notice; and
 - c. The reason for the failure.
 - d. Documentation must be placed in the individual's medical file.
5. Review of Notice. The Privacy Committee will meet quarterly basis to discuss practice adherence to the Notice and to identify any necessary updates or changes to the Notice.
6. Changes to the Notice. The practice is required to abide by the terms of the Notice, which is currently in effect. The practice reserves the right to change the terms of the notice and to make the new Notice provisions effective for all personal health information the practice already has about an individual and may obtain in the future.
- a. The practice must post any changes to the Notice thirty (30) days prior to making the change effective.
 - b. All revised notices will be promptly posted and made available to individuals in the reception area and on the practice Web Site.
 - c. Changes to the Notice will only be effective on the date that is reflected at the bottom of the last page on the revised Notice.
 - d. Business Associates who handle PHI for or on behalf of the practice must be provided with an updated Notice within seven business days of the effective date of the updated Notice.
7. Notice Requests. Individuals may request a current Notice when he/she visits the office. A current Notice must be kept at the reception desk and provided to individuals upon request.
8. Practice Contact. If an individual would like more information about the Notice, *Dr. Dobozi* will receive and process all requests at 212-826-0815.
9. Compliance. Employees have a duty to comply with the policies and procedures set forth by the practice. Any employees found to violate the practices' policies and procedures are subject to disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.

ATTACHMENT A

Bruce S. Dobozi, M.D. Allergy & Asthma
121 East 60th St, New York, NY 10022
Phone: 212-826-0815/Fax: 212-826-0819/Email: bdobozi@earthlink.net

Notice of Privacy Practices

I, _____, acknowledge that I have received the Notice of Privacy Practices.

Signature

Date

Bruce S. Dobozi, M.D. Allergy & Asthma
121 East 60th St, New York, NY 10022
Phone: 212-826-0815

**Notice of Privacy Practices
Summarized**

Our practice is required by law to follow the practices described in this summary. This is a summary of our Privacy Practices, but does not replace the full version, which you have also received. This notice describes how medical information about you may be used and disclosed and how you can get access to this information. This notice applies to personal health information that we have about you, and which are kept in or by our medical practice. Neither this summary nor the full Notice of Privacy Practices covers every possible use or disclosure. If you have any questions, please contact the Privacy Officer for this medical practice.

Who has access to your personal information?

We may use your personal health information to:

Plan your treatment and services.

Submit bills to your insurance, Medicaid, Medicare, or third party payer.

Obtain approval in advance from your insurance company to determine whether payment for the treatment is covered by your plan or to facilitate payment of a referring physician.

Perform healthcare operations such as sharing your information with business associates who need to use or disclose your information to provide a service for our medical practice (such as our billing company).

Exchange information with other State agencies as required by law.

Treat you in an emergency.

Treat you when there is something that prevents us from communicating with you.

Send you appointment reminders.

For certain types of research.

When there is a serious public health or safety threat to you or others.

To agencies involved in a disaster situation.

As required by State, Federal, or local law. This includes investigations, audits, inspections, and licensure.

To law enforcement if you are a victim of a crime, involved in a crime at our facility, or you have threatened to commit a crime.

To coroners, medical examiners, and funeral homes when necessary for them to do their jobs.

When ordered to do so by a court.

To Federal officials involved in security activities authorized by law.

To the correctional facility if you are an inmate.

Patient Rights.

As a patient in our practice you have the right:

To ask that we communicate with you about medical matters in a certain way or at a certain location. This must be made in writing.

To inspect and get a copy of your record (with some exceptions).

To appeal if we decide not to let you see all or some parts of your record.

To ask for the record to be changed if you believe you see a mistake or something that is not complete. You must make this request in writing. We may deny your request if:

We did not create the entry that is wrong; or

- the information is not part of the file we keep; or
- the information is not part of the file that we would let you see; or we believe the record is accurate and complete.

To limit how we use or disclose information about you. For example – not to release information to your spouse or a particular provider agency. This must be made in writing, and we are not required to agree to the request.

To know to whom we have sent information about you for up to the last six years. The first request in a 12 month period is free. We may charge you for additional requests.

To have a paper copy of the Notice of Privacy Practices.

To file a complaint if you believe any of your rights have been violated. All complaints must be in writing. You will not be penalized if you file a complaint.

To tell us (authorize) other releases of your personal information not described above. You may change your mind and remove the authorization at any time (in writing).

If you wish to exercise any of these rights, or to file a complaint, you should contact the Privacy Officer of this medical practice.

Bruce S. Dobozi, M.D. Allergy & Asthma
121 East 60th St, New York, NY 10022
Phone: 212-826-0815

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.

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), you have a right to adequate notice of the uses and disclosures of your protected health information (“PHI”) (i.e., information that discloses your identity or leads to disclosure of your identity) that may be made by this medical practice. You are also entitled to notice of your rights and the duties of this practice with respect to your personal health information.

Optional: You may want to include a mission statement here describing your thoughts about your patient’s personal health information. For example: “We respect your right to privacy and understand that your medical information is personal to you. In order to provide medical services to you, we create paper and electronic records about your health and the care we provide. Your personal health information is confidential and this notice is intended to help you understand how our practice uses and discloses your personal health information and what rights you have with respect to your medical information.”

Required by Law

Our practice has the following duties with respect to your personal health information:

- 1) We are required by law to maintain the privacy of your personal health information.
- 2) We must provide you with notice of our legal duties and privacy practices with respect to personal health information.
- 3) We must abide by the terms of the notice of privacy practices that is currently in effect.

How We May Use and Disclose Your Information

The following describes how our practice is permitted by law to share your personal health information with others in order to provide you with medical care. This notice does not describe every use or disclosure our practice makes; it is intended as a general overview.

Medical Treatment. We may need to share information about you in order to provide medical care to you. For example, we may share information with other physicians, nurses or healthcare professionals entering information into your medical records relating to your medical care and treatment. We may share information about you including x-rays, prescriptions and requests for lab work.

Payment. We may need to disclose information about the treatment, procedures or care our practice provided to you in order to bill and receive payment for services we provided. We may

share this information with you, an insurance company or any third party responsible for payment. We may also need to disclose personal health information about you with your health plan and/or referring physician in order to obtain prior authorization for treatment, to determine whether payment for the treatment is covered by your plan or to facilitate payment of a referring physician.

Healthcare Operations. In order to help us run our practice more efficiently and provide better patient care, we may use and disclose your personal health information to Business Associates who need to use or disclose your information to provide a service for our medical practice, such as our billing company or software vendors who provide assistance with data management on our behalf. *[Provide additional examples appropriate to your practice].*

Required by Law. We will disclose medical information related to you if required to do so by state, federal or local law.

Public Health Activities/Risks. Your medical information may be disclosed to a public health authority that is authorized by law to collect or receive such information for public health activities. Certain disclosures may be made for public health activities in the following circumstances:

- 1) to prevent or control disease, injury or disability;
- 2) to report of births or deaths;
- 3) to report child abuse or neglect;
- 4) to report reactions to medications or product defects;
- 5) to notify individuals of product recalls;
- 6) to notify a person who may have been exposed to a communicable disease or at risk of contracting or spreading a disease or condition;
- 7) if our practice reasonably believes a person is the victim of abuse, neglect, or domestic violence, we may disclose personal health information to the appropriate authority. We will only make this disclosure if you agree to the disclosure or we are required or authorized to do so by law without your permission.

Appointment Reminders or Treatment Alternatives. Our practice may use and disclose medical information about you to provide you with reminders that you are due for care or you have an upcoming appointment. We may also wish to provide you with information on treatment alternatives or other health related benefits that may be of interest to you. We may contact you by phone, fax or e-mail. We will make every effort to protect your privacy when leaving a message for you and try to reveal as little confidential information as possible (e.g., when leaving a message on your answering machine that may be heard by others).

Research. Under certain circumstances, our practice may use or disclose your personal health information for research purposes. Our practice cannot use or disclose information about you without your written authorization, but we may if the authorization requirement has been waived by a Review Board who has assessed the effect of the research protocol on your privacy rights and interests and certified that there are adequate controls in place to protect your information from improper use and disclosure. Our practice may also disclose information about you in preparing to conduct research (e.g., to help them find patients who may be qualified to participate in a particular study), but your information will not leave our practice. We will make all attempts to make your information non-identifiable, but we may not always be able to

guarantee this. If however, the researcher will have access to information that will identify you, we will seek to obtain your permission (though we cannot guarantee this). We will always obtain your specific authorization if required by law.

To Avert Serious Threat to Health or Safety. If our practice believes, in good faith, that a use or disclosure of your medical information is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, we may disclose your medical information.

Worker's Compensation. We may release medical information about you for work-related illness or injury for workers' compensation or other related programs.

Health Oversight Activities. Your personal health information may be disclosed to federal, state or local authorities as part of an investigation or government activity authorized by law. This may include audits, civil, administrative or criminal investigations, inspections, licensure or disciplinary actions or other activities necessary for the oversight of the health care system, government benefit programs and compliance with government regulatory programs or civil rights laws.

Law Enforcement. We may disclose your personal health information to law enforcement individuals if we are required to do so by law. We may also disclose medical information about you in compliance with a court order, warrant or subpoena or summons issued by the court. We will make best efforts to contact you about these types of requests so that you can obtain an order restricting or prohibiting disclosure of the information requested. We may also use such information to defend ourselves in actions or threatened actions that may be brought against our practice.

Coroners, Medical Examiners and Funeral Directors. We may release personal health information to a coroner or medical examiner for the purposes of identification, determining cause of death or other duties as authorized by law. We may also release medical information to funeral directors as necessary to carry out their duties with respect to the deceased.

Organ, Eye, Tissue Donation. If you are an organ donor, we may disclose your personal health information to organ procurement organizations, or other entities that facilitate tissue donation or transplantation.

Inmates. If you are an inmate of a correctional institution or within the custody of law enforcement officials, we may disclose medical information about you to allow the institution to provide you with medical care, to protect the health and safety of yourself and others, or for the safety and security of the correctional institution.

Other uses and disclosures will be made only with your written authorization and you may revoke your authorization at any time.

[Please Note: *If a use or disclosure for any purpose as described above is prohibited or materially limited by other applicable law (e.g., state law), the description of such use or disclosure must reflect the more stringent law.]*

Uses and Disclosures Where We Will Obtain your Written Authorization

Psychotherapy Notes. We may only disclose your psychotherapy notes for limited purposes such as carrying out treatment. For other purposes we will obtain your written consent.

Marketing. For most marketing purposes we will obtain your written consent; exceptions include if the product or service is directly treatment related, discussed face-to-face or given as a promotional gift of nominal value.

Uses and Disclosures That You Can Agree or Object To

Others Involved in your Healthcare. Unless you object, we may 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. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.

Emergencies. We may use or disclose your protected health information in an emergency treatment situation. If this happens, your physician shall allow you to object to future disclosures as soon as reasonably practicable after the delivery of treatment.

Patient Rights

You have the following rights with respect to your personal health information:

Right to Receive Personal Health Information Confidentially. You have the right to receive confidential communications of your personal health information by alternate means or at alternate locations. For example, if you would like for us only to communicate with you at home, and never at your workplace or to send information to you on your workplace e-mail, you may request this of our practice. You must make this request in writing but do not need to disclose the reason for your request. We will attempt to accommodate all **reasonable** requests. Please be specific as to how or where you wish us to communicate with you.

Right to Inspect and Copy. You have the right to inspect and copy your medical record that has been created to treat you and is used to make decisions about your care. This includes medical and billing records. Records related to your care may also be disclosed to an authorized person such as a parent or guardian upon proper proof of a legitimate legal relationship. You must submit your request in writing to inspect and copy your records. If you would like to copy your records, our practice may charge you fees for the cost of copying records, mail or other minimal costs associated with your request.

Right to Amend. If you think there is information in your record that may be inaccurate or incomplete, you have the right to request an amendment or clarification of information in your

record. Your request to make an amendment to your record must include the following and may be refused if the following elements are not met:

- 1) Submit your request in writing
- 2) Describe what you would like the amendment to say and your reasoning for why the change should be made
- 3) The amendment must be dated, signed by you and notarized

Please note that we will not change information created by third parties, if the information is not part of the medical information kept by our practice or we believe the information you provided to us is inaccurate or incomplete. We reserve the right to deny your request if we have reason to believe the information is accurate.

Right to Restrict Uses and Disclosures. You have the right to request restrictions on how our practice makes certain uses and disclosures of your personal health information for treatment, payment or healthcare operations. You may restrict how much information we may provide to family members regarding your treatment or payment for your care. You may also restrict certain types of marketing materials related to your care or treatment. **We are not required to agree to your request or we may not be able to comply with your request, but we will do all that we can to accommodate your request. If we agree to your request, we must comply. However, if the information is required to provide emergency treatment to you, we will not comply.** Your request must be in writing and include the following:

- 1) What information you would like to limit
- 2) Whether you want to limit our use, or disclosure or both
- 3) To whom you want the limits to apply (e.g., disclosures to parents, children, spouse, etc.)

Right to an Accounting of Uses and Disclosures. You have the right to receive an accounting of the disclosures of your personal health information that our practice makes for purposes other than treatment, payment or healthcare operations. All requests must be submitted in writing. All requests must be for disclosures dated **AFTER April 14, 2003 [or when the final privacy regulations are effective]**. All requests must state a time period **not longer than six (6) years back**. You must state whether you would like the accounting in electronic or paper form. One request in a twelve-month period will be provided to you at no charge. We may charge you a fee for all additional requests within a twelve-month period. We will notify you as to the cost of fulfilling your additional request and allow you the opportunity to modify it before fees are due.

All requests should be submitted to the reception desk for appropriate processing.

Right to Copy of Notice. You have the right to obtain a copy of our notice of privacy practices upon request at any time. Please call us at 212-826-0815 for a copy or ask for a copy at the reception desk. **[Please Note: You may provide the option to receive the notice via e-mail, but you can inform your patients they are still entitled to a paper copy if they choose this option].**

Changes to this Notice. Our practice is required to abide by the terms of this notice, which is currently in effect. We reserve the right to change the terms of this notice and to make the new notice provisions effective for all personal health information we already have about you and may obtain in the future. If we change our notice, we will post notice of this change thirty (30) days prior to making the change effective. **Changes will be posted on our practice Web site.**

All revised notices will be promptly posted and made available to you in our waiting room. You may also request a current Notice when you visit our office. Changes to our notice will only be effective on the date that is reflected at the bottom of the last page on the revised Notice.

If our privacy policy is revised you will be notified of such revision at the time of your next office visit & changes to such will be posted on our website.

Practice Contact. If you would like more information about this notice, please contact Dr. Dobozi at 212-826-0815. If you have any complaints regarding our privacy practices, please address your complaint to Dr. Dobozi in writing and follow the designated complaint process below.

Complaints. If you believe your privacy rights may have been violated or you become aware of a privacy concern you would like to report to our practice, please follow this complaint process:

1. Send a written letter to the practice contact named above, including the following information:
 - a. Name and Address
 - b. Social Security Number or Patient Identification Number
 - c. Detailed description of the circumstances surrounding your complaint including dates, times and any relevant information to help us understand your complaint.
 - d. Contact information
 - e. Signature and Date
2. Please allow fourteen (28) business days for an answer from our practice regarding your complaint.
3. If you are not satisfied with our response to your complaint, you may notify the Secretary of the Department of Health and Human Services.

Please note, all concerns or complaints regarding your personal health information are important to our practice. There will be no retaliation against you for filing a complaint with our office.

Additional Privacy Protections. Our practice is committed to protecting your privacy and for the proper use and disclosures of your personal health information. For example, if you treat patients with particularly sensitive conditions, even though the law allows you to disclose the information for various reasons, you will not do so unless required by law.

[Optional Elements]

Electronic Notice. We are also required to prominently post our Notice of Privacy Practices on our medical practice Website. You can find this notice at <http://www.NYasthma.salu.net>

Date of Last Revision. [April 2003]

Effective Date. Immediately.

Subject: Staff Facsimile

Policy: 8

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to transmit via facsimile all communications containing protected health information confidentially and securely.

Procedures:

1. Process. Facsimile ("fax") communications containing protected health information ("PHI") may only be made to approved business associates or authorized persons or entities only.
2. Staff may not send by fax especially sensitive medical information (e.g., HIV/AIDS information, sexually transmitted diseases, etc.) without the express permission of the Privacy Officer or their designee and appropriate authorization of the person who is the subject of the record.
3. Storage. Fax machines will be stored in a secure location at all times.
4. Cover Sheet. All communications sent by staff using a fax machine must be sent with the practice fax cover sheet (See Attachment A) that contains at least the following:
 - a. Practice name, address and phone number
 - b. Clear identification of who is the intended recipient of the fax
 - c. A paragraph on the cover sheet approved by the Privacy Officer indicating that the communication is confidential privileged and intended solely for the use of the individual or entity to which it is addressed. The statement must also say if the recipient received the communication in error, they should notify the sender (hence the reason for you to provide your practice contact information)
 - d. A "Confidential" mark showing the document is clearly confidential and should be treated as such.
5. Staff must limit the information disclosed to only that information which is requested by the recipient.
6. Fax Transmission. Staff must review all fax communications to verify the intended recipient and facsimile number is correct before sending the communication.

7. If staff is sending a fax containing PHI to the business associate or entity for the first time, verify the recipient's fax machine is located in a secure location before sending.
8. Staff must program frequently used numbers into the fax machine to prevent dialing errors.
9. Staff must telephone the recipient to verify it received the fax or request a confirmation of receipt.
10. Misdirected Fax Communications. Staff must file a written report for any misdirected fax transmissions.
11. Audit. *Dr. Dobozi*n will gather fax transmission reports regularly (*weekly*) to review the transmission reports and identify any suspicious activity. Check the numbers where faxes have been sent against the practice fax log (*or other documentation identifying to whom your practice sends fax communications*).
12. Unauthorized or suspicious calls in the transmission reports will be documented and investigated by the Privacy Officer.
13. Compliance. Employees have a duty to comply with the policies and procedures set forth by the practice. Any employees found to violate the practices' policies and procedures are subject to disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.

ATTACHMENT A

FAX COVER SHEET

**Bruce S. Dobozi, M.D. Allergy & Asthma
121 East 60th St, New York, NY 10022**

Phone: 212-826-0815/Fax: 212-826-0819/Email: bdozoin@earthlink.net

Date:

To:

Company:

Fax Number:

**Phone
Number:**

From:

Re:

Pages: _____ (including cover)

Urgent

For Review

Please Comment

Please Reply

Notes:

This communication and any files transmitted with it may contain information that is confidential, privileged and exempt from disclosure under applicable law. It is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient, you are hereby notified that any use, dissemination or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender. Thank you for your co-operation.

CONFIDENTIAL

Subject: Staff E-mail

Policy: 9

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 3 (including Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), state and local laws and sound ethical business practices. It is the Practice’s policy to define the appropriate use of the Practice e-mail systems and applies to all users including, but not limited to, employees, medical staff, and contractors. This policy applies to all usage of the Practice electronic mail systems where the mail either originated at a Practice computer or network, or is received into a Practice computer or network from an external mail system. This policy assumes use of the public Internet and interaction with patients and other members of the public at large.

Procedures:

1. User Responsibilities. The User is any person who is authorized to receive, read, enter, or update information created or transmitted via the practice e-mail systems(s). E-mail may be used only in connection with the user’s job functions and for business purposes only. Users understand that all e-mail transmissions are made with permission of the practice and are identified with the practice. User agrees to use electronic mail so as not to diminish or negatively affect the image or reputation of the practice. User will not respond to e-mails without first establishing that a signed *Patient E-Mail Consent* form exists (See Attachment A), or without permission from the practice physician(s). Users are expected to use e-mail appropriately, effectively, and efficiently and will be subject to disciplinary action by the practice including but not limited to sanction, suspension or termination for failing to comply with the practice E-mail policy.
2. Prohibited E-Mail Uses. E-mail may not be used for the following purposes:
 - a. Urgent or time-sensitive communications.
 - b. Highly confidential or sensitive information, e.g., discussion of HIV status, mental illness, chemical dependency, and workers compensation claims.
 - c. The attachment of ((XXX)) files for transmission by e-mail (*describe limitations to e-mail attachments, e.g., large database files, etc.*).
 - d. Marketing purposes without explicit permission from the target recipient.
 - e. Communication via your professional e-mail account with family members.
 - f. Personal use.

This list is not inclusive and is subject to change on notice by the practice. All questions related to the prohibited uses of e-mail should be directed to the Security Officer.

3. Employee Privacy of E-Mail. The practice recognizes that users have some expectation of privacy with respect to the e-mail received and/or stored on the practice system. However, the practice reserves the right to access the electronic mail system for legitimate business interests and to ensure the proper utilization of its property. The practice may access the e-mail system to locate and retrieve lost messages; perform duties when an employee is out of the office or otherwise unavailable; maintain control of the system by analyzing message patterns and implement revisions as needed; recover from systems failures and other unexpected emergencies; and investigate suspected breaches of security or violations of policy with probable cause. The Security Officer or designate prior to accessing an employee's files will approve any review of an employee's messages.
4. E-Mail Confidentiality and Security. E-mail is subject to the same or greater security and confidentiality protections that apply to written documents. It is the policy of this practice to protect the privacy and confidentiality of any information of a confidential or sensitive nature received or transmitted via electronic mail. This also applies to any messages transmitted through forwarding, printing, and circulating via e-mail.
5. Security Measures. The practice uses the following security measures when e-mail is used for the communication of confidential or sensitive information (e.g., patient information, personnel actions, sensitive business/legal information):
 - a. Encryption during the transmission of data for any information considered confidential or sensitive. This can be accomplished by either using the internal encryption capability built into the practice software or by using some other approved encryption system and/or service. The use of encryption may be waived only at patient's insistence. Documentation of this waiver must be kept on file. Under no circumstances may unencrypted wireless communications be used with patient-identifiable information. Any questions related to encryption should be directed to the Security Officer.
 - b. All members of the practice use password protection for access to practice systems prior to the use of practice e-mail and password protected screen-savers.
 - c. Access to and the use of e-mail communications is defined on a role based standard limiting access to e-mail based on the employee's job function.
 - d. Patient-identifiable information may never be forwarded to a third party without patient's written permission.
 - e. Any information transmitted via e-mail that is highly confidential or of a sensitive nature must be accompanied by the word "SENSITIVE" in the subject line of the e-mail to further safeguard the confidentiality of electronically submitted data.
 - f. The subject line "TO" will be viewed prior to sending all messages to ensure the message is for the intended recipient.
 - g. The practice prohibits the use of a distribution lists for the transmission of confidential or sensitive information. Confidential or sensitive information is to be distributed only to those for which there is a legitimate business interest. All information distributed to multiple recipients must be sent by blind message only.
 - h. Printers must operate in an area that is accessible to staff only and not to patients.

- i. Computer access and e-mail rights will be terminated immediately upon separation of employment with the practice.
- j. Patient e-mail shall never be used in any marketing related activities.

All questions as to the propriety of transmitting confidential or sensitive information shall be directed to the Security Officer.

6. E-mail Retention. Electronic mail used in a clinical setting constitutes a form of progress note. In the absence of an electronic patient record that allows inclusion of e-mail messages, each e-mail message should be printed in full and a copy placed in the patient's paper record. Efficient archiving can be accomplished by doing the following:
 - a. Including the full text of the patient's query in the e-mail reply.
 - b. Copying (cc:) the reply to the sender.
 - c. Printing the sender's copy (which includes the initial message and reply) and file it in the patient record unless an acknowledgement is expected. When such an acknowledgement has been requested, e.g., when important medical advice has been given, the printed (chart) copy should not be filed until this confirmation is received.
7. Backups. The practice will perform (*weekly*) backups of mail onto long-term storage (as applicable to paper records) and will store the records for *6 years* on back-up systems. The practice maintains an e-mail repository *on local machines*. *Dr. Dobozi* will clear e-mail from the archive server/s *annually*.
8. Compliance. Employees have a duty to comply with the policies and procedures set forth by the practice. Any employees found to violate the practices' policies and procedures are subject to disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.

ATTACHMENT A

Bruce S. Dobozi, M.D. Allergy & Asthma
121 East 60th St, New York, NY 10022
Phone: 212-826-0815/Fax: 212-826-0819/Email: bdozozi@earthlink.net

Patient E-Mail Consent Form

The practice of Bruce S. Dobozi, M.D. [Allergy & Asthma] does not in general offer patients the benefit of communication via e-mail. In addition to personal and telephone discussions, I (Patient Name) would like to use e-mail as a method of communication with the Practice and have read and understand the following:

Privacy. I understand that e-mail may be used only for non-emergency questions and requests in the ordinary course of business and, as a result, persons employed by the practice will be responsible for access to and processing such communications. The following staff members and physician(s) will have the right to access e-mail communication received by the practice:

Table with 2 columns: Name, Purpose. Includes four rows of blank lines for entry.

I understand that confidential and sensitive information will never be shared with a third party without my written authorization. I also understand that there are certain situations in which Dr.(s) _____ may share my e-mail messages without written authorization (e.g., disclosures required by state or federal law). I also understand that if law requires a disclosure, only the minimum amount of information necessary to achieve the purpose of the request will be disclosed. Subsequently, I will receive notice that the disclosure was made.

Response Time. The Practice will make every effort to respond to your e-mail request within (2-3 business days is suggested). If, for any reason (such as vacation, illness, emergency), I am unavailable to answer your e-mail request within the designated timeframe, you will receive a response from another physician or employee from the practice authorized to address your e-mail.

Users will receive an automatic reply message from the practice to confirm receipts of an e-mail message. The message will state the expected office response time and include contact information if you need immediate assistance.

Permissible Uses. The Practice will allow e-mail use for medical advice and non-urgent or non-emergency matters including:

Table with 2 cells: Appointments, Billing/Insurance questions

Non-Permissible Uses. Prohibited uses of e-mail include but are not limited to:

- 1) Urgent or time-sensitive communications
- 2) Highly confidential or sensitive information, e.g., discussion of HIV status, mental illness, chemical dependency and workers compensation claims
- 3) Using e-mail to attach large database files or files containing inappropriate materials unrelated to the permissible uses defined above

If the practice feels the content or subject matter of an e-mail is inappropriate for an electronic response, it reserves the right to refuse communication via e-mail and will suggest alternate means to discuss the question or request. I understand that at no time should I expect a diagnosis, a recommendation of treatment or a prognosis via e-mail regarding a complaint or symptom for which the physician did not see me personally, regardless of whether the physician has seen me personally on prior occasions.

I understand that at any time the Practice may terminate e-mail communications with me and that I will be notified of such termination by (*List Manner of Notification*). I understand that termination of online communication does not necessarily mean termination of the patient-physician relationship.

Patient Responsibilities. I understand that e-mail should be used only for appropriate messages and non-urgent situations. I agree to call the practice immediately if the situation escalates to a point where a phone call or visit is necessary. I also agree to do the following when making an e-mail request:

- 1) Choose the category of the transaction offered (e.g., prescription, appointment, medical advice, billing question).
- 2) Place my full name and patient ID in the first line of the body of the message.
- 3) Configure automatic reply to acknowledge receipt of the message, if possible.

I also understand that all messages, with replies and confirmation of receipt will be printed and placed in the patient's medical record, and it is the patient's duty to maintain their own copies of e-mail communications.

Security. The Practice has the following security mechanisms in place to secure confidential and sensitive information (*your practice should have the following listed below, insert other measures used by the practice*):

- 1) Encryption will be used for all messages when practical and always for confidential or private information.
- 2) Back-ups of data will be performed (*<insert>e.g., weekly, monthly*) onto (*<insert>long-term storage, secure site*).
- 3) Password protection allows access only to authorized users permitted to access and handle all office e-mail communications.
- 4) Password protected screen savers will be used on computers, including keeping all screens out of public view.
- 5) Information sent in a group mailing will maintain the confidentiality of the patient by using a blind copy to keep recipients invisible to each other.

Indemnification. You agree to indemnify, defend and hold harmless **Bruce S. Dobozi, M.D. [Allergy & Asthma]** its officers, directors, employees, agents and independent contractors from and against any and all losses, expenses, damages and costs arising out of your use of Patient e-mail, any activity related to your patient account information and any information lost due to technical failures.

Consent

I have read this consent, have been given the opportunity to discuss the issues with the practice and understand that by signing this consent I agree to the above policy and conditions established by this practice. I understand that I may also withdraw consent for the use of e-mail interactions at any time without affecting my right to future treatment.

Patient Name

Date

Patient's Legal Representative

Date

Subject: Appropriate Safeguards

Policy: 10

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**’s policy to provide the appropriate safeguards to protect the privacy of protected health information.

Procedures:

1. General Requirements. **Bruce S. Dobozi, M.D. [Allergy & Asthma]**’s practice will implement the “appropriate administrative, technical and physical safeguards to protect the privacy of protected health information” as required by the Final Privacy Rule.
2. Incidental Disclosures. Incidental uses and disclosures of protected health information (e.g., calling out a patients name in the waiting area) are acceptable provided that the practice has implemented the safeguards required by the Final Privacy Rule pursuant to §164.530(c), and the requirements under the “minimum necessary” standard.
3. Determining Appropriateness. To determine what is “appropriate” for a given practice, the department uses the standard of “reasonableness.” For example, the Office of Civil Right’s Guidance includes a description of safeguards for patient charts placed outside examining rooms:
 - a. “Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting patient access to certain areas, ensuring that the area is supervised, escorting non-employees in the area or placing the patient chart in the box with the front cover facing the wall. Each covered entity must evaluate what measures are reasonable and appropriate in its environment.”
OCR Guidance page 18.

Policies and Procedures Recommended to Implement the Standard [Practice Must Customize]

While policies and procedures may themselves be considered administrative safeguards, one should not overlook that policies and procedures may be necessary to fully implement physical and/or technical safeguards. For example: locks on medical records rooms may be a physical safeguard but covered entities will most likely have to implement a policy that establishes when the medical records room will be locked and unlocked, and who will have access to the keys and/or combinations; user ID’s and passwords to software systems may be technical safeguards but

covered entities will most likely have to implement a policy that requires employees not share ID's and passwords, and periodically change passwords.

Because of the scalability of the standard, and the subjective nature of determining what is "reasonable", it is impossible to prescribe exactly what policies and procedures a given covered entity may have to implement. As with the other safeguards, covered entities will have to perform their own assessment of what protected health information they hold, and determine what policies and procedures are reasonable to protect that information from improper use or disclosure.

Subject: Business Associates

Policy: 11

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 4 (Attachments A and B)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, specifically the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to disclose protected health information only to those business associates who will provide the practice with contractual assurances that it will maintain the privacy, confidentiality and security of the protected health information it handles in the performance of services for or on behalf of the practice.

Procedures:

1. Business Associates. A business associate is a person who performs certain functions, activities or services for or on behalf of the practice, involving the use of protected health information (PHI).
2. Examples of Business Associates. Access to PHI should only be granted to parties who have a contractual relationship with the practice and that have a business need to access the information in order to perform services for or on behalf of the practice.
 - a. Billing service/agency
 - b. Collection agency
 - c. Accountant/consultant who needs access to PHI
 - d. Answering service
 - e. Lockbox service
 - f. Transcription service
 - g. Practice management software vendor
 - h. Electronic medical records software vendor
 - i. Hardware maintenance service
 - j. Off-site record storage
 - k. Record copying service
 - l. Other independent contractors who provide business/administrative services on-site
3. Entities or Persons Not Business Associates. Businesses, persons or vendors are not considered business associates if they do not have access to PHI. For example:
 - a. The most common example is janitorial services, which do not require use or disclosure of PHI to perform their function or activity. These parties should not execute a business associate contract and should not use or disclose PHI.
 - b. Legal services provided by a regulatory attorney to a medical practice. To the degree that such services do not include the disclosure of PHI, the attorney is not a business

associate. However, legal services provided by a malpractice attorney will more likely involve the disclosure of PHI and therefore be more likely to characterize the malpractice attorney as a business associate of the medical practice.

4. Persons/entities who participate in the treatment of patients are not considered to be business associates of the practice and no business associate agreement is necessary.
5. Business Associate Contracts. **Bruce S. Dobozi, M.D.** will be responsible for gathering all contracts with third party businesses, persons or vendors and storing them in a secure location. Contracts where PHI is shared with the third party business associates should be maintained together.
 - a. The practice may not enter into new business relationship with a third party to handle PHI for or on behalf of the practice if the third party will not agree to the contractual requirements provided by the Final Privacy Rule (See Attachment A).
 - b. The practice may not continue a business relationship with a third party business associate who will not agree to incorporate the Final Privacy Rule contract provisions into a new or existing contract when renewing or renegotiating existing contracts. An alternate business associate must be found if this event occurs.
6. Transition Period. The Final Privacy Rule created a transition period allowing medical practices to operate under existing contracts for up to one year past the April 14, 2003 deadline (until April 14, 2004) only if the following circumstances are met:
 - a. The contracts are written (does not apply to oral contracts or contracts not in writing) and were executed before October 15, 2002; and
 - b. The contract was not renewed or modified after October 15, 2002 and before the Privacy Rule's final compliance date of April 14, 2003.
 - c. If these circumstances are not met the contract must be amended prior to the April 14, 2003 deadline to meet the Final Privacy Rule.
7. New Agreements. **Bruce S. Dobozi, M.D.** will be responsible for determining whether a business associate agreement is necessary. All written agreements entered into with a business associate must contain all of HIPAA's required contractual assurances (See Attachment A).
 - a. The Final Privacy Rule requires the practice to enter into written contracts with all business associates who handle PHI on or on behalf of the practice.
 - b. A written contract must be executed before the practice can disclose the PHI to the business associate.
8. Existing Agreements. **Bruce S. Dobozi, M.D.** will be responsible for reviewing all existing agreements to identify whether they must be amended to reflect the Final Privacy Rule. **Bruce S. Dobozi, M.D.** will oversee the renegotiation and/or revision of existing contracts to include the business associate contract requirements as required by the Final Privacy Rule (See Attachment B).
9. For all contracts entered into before October 15, 2002 that qualify for the transition period (allowing the practice to continue under the contract until April 14, 2004) but do

not contain any of HIPAA's required contractual provisions, the contracts will be deemed in compliance with the business associate rule until:

- i. The date the contract is renewed or modified if this occurs after April 14, 2003; or by;
 - ii. April 14, 2004.
 - iii. Existing contracts that qualify for the transition period must meet HIPAA's business associate requirements by April 14, 2004.
 - iv. **Bruce S. Dobozi, M.D.** will be responsible for identifying all contracts that must be reopened and renegotiated to meet this deadline.
10. Contracts Up for Renewal. Identify the date when the contracts are up for renewal.
 - a. If the contract renews beyond April 14, 2003, the practice can wait until the date the contract is up for renewal to amend it to meet HIPAA's business associate requirements.
 - i. For example, if the contract comes up for renewal in December 2003 - at that time the practice will discuss with the business associate the necessary contractual provisions that must be added to the existing contract and the practice will not be in violation of HIPAA.
 - b. In cases where contracts automatically renew (a.k.a. "evergreen contracts") without any change in terms or other action by the medical practice or business associate, the contracts are eligible for the extension and deemed compliance will not terminate when these contracts automatically roll over.
 - i. Evergreen contracts must be updated by the April 14, 2004 deadline.
11. **Bruce S. Dobozi, M.D.** will work with the appropriate parties and/or outside counsel as necessary to oversee the execution of business associate contracts.
12. Wrongful Activity by Business Associate. All staff must report knowledge of wrongful activity or failure by a business associate to meet its contractual obligations. If staff is aware that a business associate is failing to meet its contractual obligation to only use the protected health information for the purposes of the contract, or failing to protect the information from misuse, the practice has a duty to do the following:
 - a. Take "reasonable steps" to cure such breaches.
 - b. If the breach is not being addressed or cannot be cured, the practice must terminate the contract, if feasible.
 - c. If termination is not feasible because there are no other business alternatives, the Privacy Officer must report the problem to the U.S. Department of Health and Human Services.
13. If staff has credible evidence that a business associate is violating the terms of the contract and putting the PHI at risk, the practice must act upon such knowledge at the direction of the Privacy Officer, investigate the problem and mitigate any harm that may result.
14. Compliance. Employees have a duty to comply with the policies and procedures set forth by the practice. Any employees found to violate the practices' policies and procedures are subject to disciplinary action or corrective measures, including but not limited to,

education and awareness training, reassignment, additional supervision, disciplinary actions such as warnings, suspension or termination of employment.

Note: Certain parties that may have incidental access to PHI, such a facility-cleaning contractor, are not business associates. However, your practice should create a process for incorporating strong confidentiality provisions in agreements with these vendors.

ATTACHMENT A

BUSINESS ASSOCIATE LANGUAGE

Footnotes are included to provide further explanation to the reader and are not intended to be included in the contractual provisions.

Definitions¹

Catch-all definition:²

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule.

Examples of specific definitions:

(a) *Business Associate*. ``Business Associate" shall mean *[Insert Name of Business Associate]*.

(b) *Covered Entity*. ``Covered Entity" shall mean **Bruce S. Dobozi, M.D. [Allergy & Asthma]**.

(c) *Individual*. ``Individual" shall have the same meaning as the term ``individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(d) *Privacy Rule*. ``Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

(e) *Protected Health Information*. ``Protected Health Information" shall have the same meaning as the term ``protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(f) *Required By Law*. ``Required By Law" shall have the same meaning as the term ``required by law" in 45 CFR 164.501.

(g) *Secretary*. ``Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Obligations and Activities of Business Associate³

(a) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law.⁴

(b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

¹ These definitions are optional and may vary depending on your agreement. Headings underlined and in bold should exist as sections in your agreement.

² This "catch-all phrase" can be included in the definitions section of your agreement as a general statement to ensure that terms used by both parties, although not addressed in the agreement, will have the same meaning.

³ This section should clearly define the responsibilities of your business associate with respect to the personal health information it is handling on behalf of your medical practice.

⁴ "Required by Law" is capped throughout the Agreement if this term is defined in your definition section.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement. *[This provision may be included if it is appropriate for the Covered Entity to pass on its duty to mitigate damages to a Business Associate.]*

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner *[Insert negotiated terms]*⁵, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524. *[Not necessary if business associate does not have protected health information in a designated record set.]*

(g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner *[Insert negotiated terms]*. *[Not necessary if business associate does not have protected health information in a designated record set.]*

(h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available *[to the Covered Entity, or]* to the Secretary, in a time and manner *[Insert negotiated terms]* or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner *[Insert negotiated terms]*, information collected in accordance with Section *[Insert Section Number in Contract Where Provision (i) Appears]* of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

*Permitted Uses and Disclosures by Business Associate*⁶

⁵ Parties can negotiate mutually agreeable times and conditions to allow for access to records, amendments to records and information to account for disclosures of PHI as addressed in sections (f), (g), (h) and (j). While both parties can negotiate the terms, these rights must exist to allow your medical practice comply with its obligations under the Privacy Rule.

⁶ It is important to be very specific regarding permitted uses and disclosures of the PHI you disclose to your business associate, therefore this section should contain a General Use and Disclosure provision (either a or b) as well as a Specific Use and Disclosure Provision if there are other permitted uses and disclosures that should be addressed. Business associates should never use PHI for their own independent purposes.

General Use and Disclosure Provisions [(a) and (b) are alternative approaches]

(a) Specify purposes:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity: *[List Purposes]*.

(b) Refer to underlying services agreement:

Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in *[Insert Name of Services Agreement]*, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

Specific Use and Disclosure Provisions. *[only necessary if parties wish to allow Business Associate to engage in such activities]*

(a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

(d) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502(j)(1).

Obligations of Covered Entity

Provisions for Covered Entity To Inform Business Associate of Privacy Practices and Restrictions *[provisions dependent on business arrangement]*

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.⁷

⁷ If a patient requests certain restrictions, limitations or changes regarding the use and disclosure of their PHI and your practice agrees to such a request, you must notify your business associate of the restriction so they may comply.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. *[Include an exception if the Business Associate will use or disclose protected health information for, and the contract includes provisions for, data aggregation or management and administrative activities of Business Associate].*

*Term and Termination*⁸

(a) *Term.* The Term of this Agreement shall be effective as of *[Insert Effective Date]*, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section. *[Term may differ.]*

(b) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either: (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement *[and the ___ Agreement/sections __ of the ___ Agreement]* if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) Immediately terminate this Agreement *[and the ___ Agreement/sections __ of the ___ Agreement]* if Business Associate has breached a material term of this Agreement and cure is not possible; or (3) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary. *[Bracketed language in this provision may be necessary if there is an underlying services agreement. Also, opportunity to cure is permitted, but not required by the Privacy Rule.]*

(c) *Effect of Termination.*

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health

⁸ Your practice has an obligation to take reasonable steps if you know your business associate has violated its obligations under the contract. Once you give the business associate the opportunity to remedy ("cure") a breach and the business associate continues to violate the agreement you should terminate or report the business associate to the Secretary of Health and Human Services if termination is not a viable option. Termination may not be a viable option if you have no alternate business associates available in your location to perform the services.

Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon [Insert negotiated terms] that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

Miscellaneous

(a) *Regulatory References.* A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

(b) *Amendment.* The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

(c) *Survival.* The respective rights and obligations of Business Associate under Section [Insert Section Number Related to "Effect of Termination"] of this Agreement shall survive the termination of this Agreement.

(d) *Interpretation.* Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

ATTACHMENT B

SAMPLE BUSINESS ASSOCIATE AGREEMENT

(Created as an Amendment or Addendum to an Agreement For Services Involving the Use, Creation or Transmission of Protected Health Information)

This Business Associate Agreement ("Agreement") effective on _____, 2003 ("Effective Date") is entered into by and between _____ (the "Business Associate") and **Bruce S. Dobozi, M.D. [Allergy & Asthma]** (the "Covered Entity").

RECITALS

A. The purpose of this Agreement is to comply with the Standards for Privacy of Individually Identifiable Health Information ("protected health information") published on August 14, 2002 by the Secretary of the U.S. Department of Health and Human Services ("HHS") to amend 45 C.F.R. Part 160 and Part 164 (the "Privacy Regulation") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

B. [The parties have a prior agreement dated _____ (the "Service Agreement") under which the Business Associate regularly uses and/or discloses protected health information in its performance of services for the Covered Entity] **or,**

[Covered Entity has requested Business Associate to perform the services set forth in Attachment A hereto with the condition that Business Associate agrees to abide by the requirements set forth in the Privacy Regulation.]

C. This Agreement sets forth the terms and conditions pursuant to which protected health information that is provided by, or created or received by, the Business Associate from or on behalf of the Covered Entity will be handled.

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements hereinafter addressed, the parties agree as follows:

DEFINITIONS

Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

Required By Law. ``Required By Law" shall have the same meaning as the term ``required by law" in 45 CFR 164.501.

Secretary. ``Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

TERMS

1. Services. The Business Associate provides services for the Covered Entity that involve the use and disclosure of protected health information which services are described in Attachment A hereto. Except as otherwise specified herein, the Business Associate may make any and all uses of protected health information necessary to perform its obligations as set forth in Attachment A and/or under the Services Agreement between the parties. Additionally, Business Associate may disclose protected health information for the purposes authorized by this Agreement only (a) to its employees, subcontractors and agents, in accordance with Section 2(b), or (e) as directed by the Covered Entity.

2. Responsibilities of Business Associate. With regard to its use and/or disclosure of protected health information, the Business Associate hereby agrees to do the following:

(a) Use and/or disclose the protected health information only as permitted or required by this Agreement or as otherwise required by law;

(b) Report to the designated privacy officer of the Covered Entity, in writing, any use and/or disclosure of the protected health information that is not permitted or required by this Agreement of which Business Associate becomes aware within fifteen (15) days of the Business Associate's discovery of such unauthorized use and/or disclosure;

(c) Use appropriate safeguards including commercially reasonable efforts to maintain the privacy and security of the protected health information and to prevent unauthorized use and/or disclosure of such protected health information;

(d) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of protected health information by Business Associate in violation of the requirements of this Agreement.

(e) Require all of its employees, representatives, subcontractors or agents that receive or use or have access to protected health information under this Agreement to agree in writing to adhere to the same restrictions and conditions on the use and/or disclosure of protected health information that apply herein, including the obligation to return or destroy the protected health information as provided under (i) of this section.

(f) Upon written request, make available during normal business hours at Business Associate's offices all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Covered Entity within (____) days for purposes of enabling the Covered Entity to determine the Business Associate's compliance with the terms of this Agreement;

(g) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the Covered Entity's compliance with the Privacy Regulation, subject to attorney-client and other applicable legal privileges.

(h) Within forty five (45) days of receiving a written request from the Covered Entity, provide to the Covered Entity such information as is requested by the Covered Entity to permit the Covered Entity to respond to a request by the subject individual for amendment and accounting purposes of the disclosures of the individual's protected health information in accordance with 45 C.F.R. §164.526 and §164.528;

(i) Return to the Covered Entity or destroy, as requested by the Covered Entity, within (___) days of the termination of this Agreement, the protected health information in Business Associate's possession and retain no copies or back-up tapes; and

(j) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528; and

3. Responsibilities of the Covered Entity. With regard to the use and/or disclosure of protected health information by the Business Associate, the Covered Entity hereby agrees:

(a) To notify the Business Associate of any changes in the form of notice of privacy practices that the Covered Entity provides to individuals pursuant to 45 C.F.R. §164.520 and provide the Business Associate a copy of the notice currently in use;

(b) To notify the Business Associate of any changes in, or withdrawal of, the consent or authorization provided to the Covered Entity by individuals whose protected health information may be used and/or disclosed by Business Associate under this Agreement pursuant to 45 C.F.R. §164.506 or §164.508; and

(c) To notify the Business Associate, in writing and in a timely manner, of any restrictions on the use and/or disclosure of protected health information agreed to by the Covered Entity as provided for in 45 C.F.R. §164.522.

4. Mutual Representation and Warranty. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

5. Term and Termination.

(a) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

(b) Termination. As provided for under 45 C.F.R. §164.504(e)(2)(iii), the Covered Entity may immediately terminate this Agreement and any related agreement if it determines that the Business Associate has breached a material provision of this Agreement. Alternatively, the Covered Entity may choose to: (i) provide the Business Associate with (___) days written notice of the existence of an alleged material breach; and (ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement. If termination is not feasible, the Covered Entity shall report the breach to the Secretary of HHS. This Agreement will automatically terminate without any further action of the parties upon the termination or expiration of the Service Agreement between the parties.

(c) Effect of Termination. Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all protected health information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the protected health information.

i. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. Upon written notification that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2(d) and 2(i) and 9 shall survive the termination of this Agreement indefinitely.

7. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

8. Amendment. This Agreement may not be modified or amended, except in writing as agreed to by each party. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

9. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

10. Notices. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to Business Associate:

If to Covered Entity:

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of the ____ day of _____, 2003.

IN PRESENCE OF:

Business Associate

Witness

By: _____
Name: _____
Title: _____
Date: _____

Witness

Covered Entity

By: _____
Name: _____
Title: _____
Date: _____

Subject: Training

Policy: 12

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 1 (Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, specifically the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**’s policy to periodically train all staff on the legal and ethical requirements of patient privacy and confidentiality of the protected health information handled by this practice.

Procedures:

1. Staff Training. All staff of the practice receive privacy and security training (See Attachment A).
 - a. All new staff will undergo initial training within two weeks of their date of hire.
 - b. All existing staff whose job responsibilities change to include access to and the handling of protected health information (“PHI”) will undergo training within two weeks of change in job responsibilities.

2. Content of Training. This initial training will include at least the following:
 - a. A review of **Bruce S. Dobozi, M.D. [Allergy & Asthma]**’s Policy and Procedure Manual prior to actually handling any PHI.
 - b. A review of appropriate information practices specific to the job responsibility performed by the employee.
 - c. The following videotapes and on-line teaching tools will also be reviewed:
[Add any videotapes and on-line teaching tools that your practice uses, if any]
 - d. Training and orientation on the use of the **Bruce S. Dobozi, M.D. [Allergy & Asthma]** computer system.
 - e. Education regarding privacy and security issues relevant to personal health information as directed by the **Bruce S. Dobozi, M.D. [Allergy & Asthma]** Privacy and/or Security Officer.
 - f. Training regarding **Bruce S. Dobozi, M.D. [Allergy & Asthma]**’s Privacy Policy and the protection of confidential health information.
 - g. *(Add additional training topics as applicable to the practice)*

3. Re-training. Staff will undergo re-training as need to assure that staff has current knowledge regarding PHI privacy and security issues. In any event, staff will be trained at least bi-annually.

4. Documentation of Training. Documentation of a completed training, as well as annual and periodic training, must be filed in the employee's personnel file.

Subject: Privacy Violations

Policy: 13

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, specifically the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is Bruce S. Dobozi, M.D. [Allergy & Asthma]'s policy to establish and apply appropriate sanctions against staff who fail to comply with the privacy policies and procedures of Bruce S. Dobozi, M.D. [Allergy & Asthma] practice.

Procedures:

1. The Final Privacy Rule regulates covered entities such as Bruce S. Dobozi, M.D. [Allergy & Asthma] medical practice and not specific members of the practice. Therefore, if a staff member makes an unauthorized disclosure of protected health information ("PHI"), the practice is liable for that disclosure under the Final HIPAA Privacy Rule.
2. Instances where Practice is Not Liable. There are two instances in which the HIPAA Privacy Rule provides that the practice will not be liable for a disclosure by staff, even though the disclosure would otherwise be impermissible:
 - a. A disclosure by a whistleblower, and
 - b. A disclosure by a member of the workforce who has been the victim of a crime.
3. When Sanctions are Necessary. Pursuant to the Final Privacy Rule, the practice must apply appropriate sanctions against staff that fail to comply with the privacy policies and procedures of the practice or with the requirements of the Final Privacy regulations.
 - a. Sanctions imposed will be appropriate to the nature of the violation.
 - i. For example, the type of sanction will vary depending on factors such as:
 1. Severity of the violation
 2. Whether the violation was intentional or unintentional
 3. Whether the violation indicated a pattern of improper use or disclosure of protected health information.
 - b. Sanctions may range from additional training, warning to termination.
4. How to Report Privacy or Security Concerns or Violations. Bruce S. Dobozi, M.D. [Allergy & Asthma] encourages staff to report privacy and/or security concerns or violations. Any staff member who believes that a privacy and/or security violation has occurred or has concerns regarding the practice's privacy practices should do the following:

- a. Immediately report the alleged act(s) or concerns to their supervisor.
 - b. Supervisors and managers who receive complaints of alleged privacy and/or security violations must report the complaint to Privacy or Security Officer immediately.
 - c. If an employee wishes to make an anonymous reporting of his/her privacy and/or security concerns, the employee may do so to the Privacy or Security Officer. The staff member should provide in sufficient detail a summary of the alleged privacy or security violations or concerns and place it in an envelope titled "Privacy or Security Officer."
 - d. The Privacy or Security Officer will promptly and thoroughly investigate all complaints in a professional and confidential manner (*Practice may designate another person, attorney, etc.*) (See Attachment A). The practice prohibits any form of retaliation against a staff member for filing a legitimate complaint under this policy or for assisting in a complaint investigation. **REGARDLESS OF THE FINDINGS OF THE INVESTIGATION, THERE WILL BE NO RETALIATION AGAINST ANY STAFF MEMBER FOR REPORTING SUCH CONCERNS OR COOPERATING WITH ANY INVESTIGATION IN GOOD FAITH.**
 - e. Whenever possible, the confidentiality of the complaint will be maintained. However, there may be instances where the details of the complaint or the identity of the complaining party must be disclosed to effectively investigate or address the complaint. In all circumstances, however, the practice will take all reasonable steps to assure that the complaining party does not suffer any reprisals or retaliation.
5. Discipline. If an investigation shows that any employee or business associate has violated the practice's policies and procedures or engaged in any unlawful activity with respect to confidential information, the practice will take appropriate disciplinary action or corrective measures, including but not limited to, education and awareness training, reassignment, additional supervision, demotion, termination of the business associate relationship and/or disciplinary actions such as warnings, suspension or termination of employment.
6. The practice will determine the level of disciplinary action or corrective measure that is appropriate to the specific situation.

ATTACHMENT A

PRIVACY OFFICER'S INCIDENT LOG

**Bruce S. Dobozi, M.D. Allergy & Asthma
121 East 60th St, New York, NY 10022**

Phone: 212-826-0815/Fax: 212-826-0819/Email: bdozobin@earthlink.net

DATE RECIEVED	NATURE OF COMPLAINT	DATE OF INVESTIGATION	RESULTS OF INVESTIGATION	SANCTIONS

Subject: Patient Complaint Process for Privacy Concerns

Policy: 14

Initial Date: October 1, 2002

Review Dates: April 1, 2003

Page: 1 of 2 (Attachment A)

Approved: Bruce S. Dobozi, M.D.

Date: April 1, 2003

Statement of Purpose and Policy:

Bruce S. Dobozi, M.D. [Allergy & Asthma] has instituted this policy as part of its Compliance Program to reflect its commitment to comply with applicable federal laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), state and local laws and sound ethical business practices. It is **Bruce S. Dobozi, M.D. [Allergy & Asthma]**'s policy to provide a complaint process to individuals who feel their privacy rights have been violated and/or the practice is not adhering to its information practices communicated to individuals via the Notice of Privacy Practices or otherwise.

Procedures:

If an individual believes their privacy rights (or those of a relative or guardian) may have been violated or an individual becomes aware of a privacy concern he/she would like to report to **Bruce S. Dobozi, M.D. [Allergy & Asthma]** practice, the following complaint process must be followed: [*Customize for your Practice*]

1. Process. Staff will instruct the individual to submit a written letter to the practice contact named above, including the following information (See Attachment A):
 - a. Name and Address
 - b. Social Security Number or Patient Identification Number
 - c. Detailed description of the circumstances surrounding the complaint including dates, times and any relevant information to help the practice understand the complaint.
 - d. Contact information
 - e. Signature and Date
2. Investigation and Resolution. The Privacy Officer will investigate and respond to all complaints.
3. Response. Practice must respond to complaint within fourteen (14) business days (*State law may require a shorter period of time*). The response must include the following:
 - a. Explanation
 - b. Remedy
 - c. Mail certified U.S. Mail return receipt requested
4. Complaint and response to complaint must be filed in the individual's file.

5. The individual has the right to file his/her complaint directly with the Secretary of U.S. Department of Health and Human Services.
6. Retaliation against any individual who has filed a concern or complaint with the practice regarding his/her personal health information is prohibited.

