

---

# HIPAA HANDBOOK

Health Insurance Portability  
and Accountability Act

---

## 2014



Virginia University  
of Oriental Medicine

9401 Mathy Drive,  
Fairfax, VA 22031

[www.vuom.org](http://www.vuom.org)

703.323-5690



TABLE OF CONTENTS

A MESSAGE FROM THE DIRECTOR OF CLINICAL OPERATIONS..... 3
GENERAL INTRODUCTION..... 4
Privacy of Patient Health Information.....4
Privacy Standards.....4
Use and Disclosure of Protected Health Information .....4
Required Administrative Procedures .....4
Establishment of Individual Rights .....4
Business Associates.....5
Security Standards.....5
Privacy Committee and Privacy Officer.....5
PATIENT RIGHTS
Notice of VUOM Privacy Practices.....6
Notice of VUOM Privacy Practices Procedures.....6
Requesting Additional Privacy Protection .....7
Requesting Additional Privacy Protection Procedures.....7
Requests by Patients to Receive Communications by Alternative
Means or at Alternative Locations .....8
Access of Patients To Their Health Information .....8
Patient Access Procedures.....8
Amending Health Information ..... 11
Amendment Procedures.....12
Accounting of Disclosures ..... 13
Procedures for Accounting of Disclosures ..... 13
USING, DISCLOSING AND REQUESTING PATIENT HEALTH INFORMATION..... 16
Permitted Uses and Disclosures of Patient Health Information With Patient Authorization..... 16
Permitted Uses and Disclosures..... 16
Permitted Disclosures..... 16
Procedures for Permitted Uses & Disclosures of Patient Health Information
Without Patient Authorization..... 16
Use and Disclosure for Purposes of Treatment, Payment and Health Care Operations ..... 18
Other Regulatory Exceptions Regarding Use and/or Disclosure ..... 19
Disclosure ..... 19
Procedures to Use or Disclose Patient Health Information Without Patient's Consent ..... 20
Procedures When the Patient's Authorization is Required..... 21
Procedures..... 25
Procedures..... 26
Procedures..... 27
WORKPLACE TRAINING AND SANCTIONS FOR FAILURE TO COMPLY
WITH POLICY AND PROCEDURES ..... 29
Procedures..... 29
BUSINESS ASSOCIATES ..... 31
Procedures..... 31
HANDBOOK ACKNOWLEDGEMENT..... 33
APPENDIX ..... 34
Notice of HIPAA Privacy Practices..... 35
Acknowledgement of Notice of HIPAA Privacy Practices..... 38
Consent Form ..... 39



## A MESSAGE FROM THE DIRECTOR OF CLINICAL OPERATIONS

Virginia University of Oriental Medicine (VUOM) recognizes the need to protect the privacy of patient health information in order to facilitate the effective delivery of health care. VUOM patients must be confident and trust that VUOM personnel will not inappropriately use or disclose patient health information. By fostering such confidence and trust, the Clinic's patients will be more likely to provide accurate and complete information about their personal health, which in turn will assist the Clinic's interns and clinic supervisors in accurately diagnosing a patient's illness or condition and treating the patient more effectively.

In response to these concerns and to comply with applicable federal and state laws, VUOM has implemented this Privacy Manual which provides guidance to VUOM personnel regarding the policies and procedures VUOM has implemented to ensure that patients are afforded their rights with respect to their health information and that VUOM personnel use and disclose such information appropriately.

All VUOM staff and interns are urged to maintain a working knowledge of the provisions of this Manual as an ongoing job duty and for the protection of the patient's privacy. It is anticipated that with a detailed knowledge of this Manual, VUOM staff and interns will be able to confidently discharge their duties to patients and to VUOM in providing the highest quality healthcare.

## GENERAL INTRODUCTION

### Privacy of Patient Health Information

Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was enacted to improve the efficiency and effectiveness of the health care system through the establishment of standards and requirements for the electronic transmission of certain health information. To achieve that end, HIPAA requires the Secretary of the U.S. Department of Health and Human Services ("Secretary") to issue a set of interlocking regulations establishing standards and protections for the health industry (collectively, the "HIPAA Standards"). The HIPAA Standards apply to Covered Entities which are defined as health plans, health care clearinghouses and those health care providers who transmit any health information in electronic form in connection with certain administrative and billing transactions.

On December 28, 2000, the Secretary published a final rule setting forth standards for the privacy of individually identifiable health information ("Protected Health Information") maintained by Covered Entities ("Privacy Standards"). This rule was subsequently revised on August 14, 2002. In addition, on August 12, 1998, the Secretary issued a final (February 20, 2003) rule setting forth standards relating to the security of health information and the use of electronic signatures by Covered Entities ("Security Standards").

### Privacy Standards

The Privacy Standards set forth general requirements relating to the use and disclosure of Protected Health Information maintained by Covered Entities. They also describe the administrative requirements a Covered Entity must implement relating to the privacy of Protected Health Information (e.g., workforce training, etc.). Finally, the Privacy Standards establish certain rights individuals have with respect to their Protected Health Information (e.g., right to access, right to request amendments, etc.). Covered Entities (excluding small health plans) must comply with the Privacy Standards by April 14, 2003.

### Use and Disclosure of Protected Health Information

Under the Privacy Standards, Covered Entities are prohibited from using (within the entity) or disclosing (outside the entity) Protected Health Information without patient authorization unless such use or disclosure falls within an exception. There are numerous use and disclosure exceptions set forth in the Privacy Standards. For example, one exception permits Covered Entities to use and/or disclose Protected Health Information without a patient's consent or authorization to carry out treatment, payment, health care operations (e.g., quality assurance, utilization review, credentialing, etc.). In addition, Covered Entities are permitted to use or disclose Protected Health Information without consent or authorization for other specified purposes (e.g., public health activities, required by law, etc.). Patient authorization is required, however, for most other uses and disclosures.

The Privacy Standards also require that when a Covered Entity uses or discloses Protected Health Information or requests Protected Health Information, it must make reasonable efforts to limit the



information to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request. This minimum necessary standard, however, does not apply to, among other things, disclosures to, or requests by, health care providers for treatment.

### **Required Administrative Procedures**

The Privacy Standards set forth specific administrative requirements a Covered Entity must implement. For example, Covered Entities are required to designate a privacy official to be responsible for the development and implementation of the Covered Entity's privacy policies and procedures. Covered Entities are also required to provide workforce training and implement specific policies and procedures designed to protect the privacy of Protected Health Information.

### **Establishment of Individual Rights**

The Privacy Standards establish certain rights individuals have with respect to their Protected Health Information. For example, under the Privacy Standards, individuals have the right to receive adequate notice of the privacy practices of a Covered Entity. Individuals also have the right to request that a Covered Entity restrict the uses and/or disclosures of their Protected Health Information. In addition, the Privacy Standards require Covered Entities to allow individuals to inspect, copy and request amendments to their Protected Health Information.

### **Business Associates**

The Privacy Standards only apply directly to Covered Entities. However, they are designed so that a Covered Entity bears the responsibility of insuring the privacy of the Protected Health Information shared between it and certain other persons who perform functions or activities on behalf of the Covered Entity ("Business Associates"). Therefore, under the Privacy Standards, a Covered Entity may only disclose Protected Health Information to a Business Associate, and may only allow a Business Associate to create or receive Protected Health Information on its behalf, if the Covered Entity obtains satisfactory assurance that the Business Associate will appropriately handle the information. A Covered Entity must document such satisfactory assurance through a written contract or agreement which contains a number of specific provisions. In addition, a Covered Entity must take certain actions if the Covered Entity learns that a Business Associate materially breaches or violates the terms of such written agreement.

### **Security Standards**

As proposed, the Security Standards require each Covered Entity to develop and employ certain security requirements. These standards generally outline the administrative procedures, physical safeguards and technical security services/mechanisms that must be developed and maintained by Covered Entities. Similar to the Privacy Standards, the Security Standards require Covered Entities to enter into agreements with their Business Associates to ensure each Business Associate maintains the same level of security in connection with Protected Health Information. In general, the proposed Security Standards are designed to address the risk of improper access to electronically stored information as well as the risk of interception of information during electronic transmission by requiring each Covered Entity to assess potential risks and vulnerabilities to the individual health data in its possession and to develop, implement and maintain appropriate security measures with respect to such data, if such data is to be transmitted via electronic means. However, the final Security Standards do not reference or advocate specific technology because security technology is changing quickly. The Secretary of HHS has indicated that Covered Entities should have the flexibility to choose their own technical solutions. The standards also do not address the extent to which a particular entity should implement specific features. Instead, HHS requires only that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. Thus, each organization must decide for itself the appropriate security measures to employ and which technology to use.

### **Privacy Officer**

VUOM is committed to protecting the privacy of the health information of its patients, ensuring that patients are afforded their rights with respect to their health information, and complying with applicable federal, state and local laws. Therefore, VUOM has established a Privacy Committee to oversee the implementation of this Privacy Policy which is designed to comply with the HIPAA Privacy Standards.

A key member of the Privacy Committee is the Privacy Officer, a position which is integral to the continuing success of VUOM's privacy efforts. The Privacy Officer is responsible for overseeing the development and implementation of corporate-wide privacy policies and procedures set forth in this Privacy Policy. The Privacy Officer is also responsible for overseeing the office that provides further information about matters covered by VUOM's Notice of Privacy Practices and receives complaints if a patient believes that his or her privacy rights have been violated.



The Privacy Officer is:

Hyung Sik Byeon, L.Ac., Director of Clinical Operations  
Virginia University of Oriental Medicine (VUOM) • Acupuncture Clinic  
9401 Mathy Dr., Fairfax, VA 22031 • (703) 323-5691 • [clinic@vuom.org](mailto:clinic@vuom.org)

## PATIENT RIGHTS

### Notice of VUOM Privacy Practices

Patients have certain rights with respect to their health information created or received by VUOM. For example, patients have the right to receive a notice of VUOM's privacy practices describing patient rights, and VUOM's legal duties, with respect to patient health information. It is the policy of VUOM that its personnel afford patients this right by complying with the procedure below.

### Notice of VUOM Privacy Practices Procedures

- 1. Delivery of Notice:** Except in an emergency treatment situation, VUOM's reception personnel shall give to each patient no later than the date of the first service delivery, including service delivered electronically, VUOM's Notice of Privacy Practices, a copy of which is attached as Appendix A to this Manual (the "Notice").
- 2. Acknowledgment of Receipt:** Each Notice given to a patient shall have attached to it a cover page entitled Patient Acknowledgment of Receipt of Notice of Privacy Practices, a copy of which is attached as Appendix A to this Manual, which the patient will be asked to date and sign at the time the patient is given the Notice. If the patient is unable or unwilling to date and sign the acknowledgment form, VUOM personnel should document in writing on the face of the acknowledgment form the reason for the inability or refusal of the patient to sign. Such reason could simply be, for example, that the patient refused to sign after being requested to do so. VUOM's duty under the law is only to make a good faith effort to obtain the acknowledgment of receipt. If the patient does not want to sign the acknowledgment form, he or she is not required to do so. The acknowledgment form should be filed in the patient record and retained for at least six (6) years from the date of first delivery of service.
- 3. Emergency Treatment Situations:** In emergency treatment situations, VUOM personnel shall give the patient the Notice as soon as reasonably practicable after the emergency treatment situation.
- 4. Alternative Means of Communicating Notice:** VUOM will consider alternative means of communicating the contents of the Notice to certain populations, such as individuals who cannot read or who have limited English proficiency.
- 5. Available on Request at Any Time:** Even if the patient has previously received a copy of the Notice, the patient remains entitled to ask for another copy at any time.
- 6. Posting of Notice:** A copy of the Notice should be posted in a clear and prominent location where it is reasonable to expect individuals to be able to read it.
- 7. Revision of Notice:** Whenever the Notice is revised, it must be made available upon request and posted as required in Section 6 above.
- 8. Availability on Web Site:** To the extent that VUOM maintains a Web site, the Notice must be placed and maintained on VUOM's Web site and be available electronically through the Web site.
- 9. Delivery and Acknowledgment By Electronic Mail:** If a patient wishes to receive the Notice by electronic mail, the patient shall submit an agreement to receive them by electronic mail in writing to the



Privacy Officer or the Privacy Officer's designee at [clinic@vuom.org](mailto:clinic@vuom.org). When the Notice has been delivered to the patient electronically, the system should request the patient to acknowledge receipt electronically. If VUOM is aware that an electronic mail transaction has failed, patient should be sent a paper copy of the Notice. A patient who has received the Notice by electronic mail retains the right to obtain a paper copy from VUOM upon request.

10. **Responsibility for Updating:** VUOM's Privacy Officer will be responsible for developing and updating, as necessary, the Notice of Privacy Practices. Page | 6
11. **Training:** Privacy Officer will be responsible for ensuring employees are trained regarding the Notice of Privacy Practices in accordance with Section V of this Manual.
12. **Patient Questions:** Patient questions related to the Notice of Privacy Practices should be directed to the Privacy Officer at [clinic@vuom.org](mailto:clinic@vuom.org).
13. **Retention of Documents:** A copy of the original form of the Notice of Privacy Practices, and each revised form, shall be retained by VUOM for at least six (6) years from the date when the version was last in effect. Copies will be maintained in the office of the Privacy Officer. Acknowledgment forms will be retained in the patient record as provided in Section 2 above.

### Requesting Additional Privacy Protection

Patients have certain rights with respect to their health information created or received by VUOM. For example, patients have the right to request that VUOM restrict certain uses and disclosures of their health information. In addition, VUOM must permit patients to request (and must accommodate reasonable requests) to receive communications regarding their health information by alternative means or at alternative locations. It is VUOM's policy that VUOM personnel afford patients these rights by complying with the procedures set forth below.

### Requesting Additional Privacy Protection Procedures

#### Requests by Patients to Restrict the Uses and Disclosures of Health Information

1. **Permitting Patients to Request a Restriction:** VUOM must permit a patient to request that VUOM restrict the following: (a) uses or disclosures of the patient's health information to carry out treatment, payment or health care operations; and (b) disclosures to family members, relatives, close personal friends and other persons assisting in the patient's care.
2. **Agreeing to a Restriction:** VUOM personnel are not required to agree to a restriction requested by the patient. However, if a member of VUOM's personnel does agree to such a restriction, all of its personnel must honor the request, except that VUOM's personnel may, in violation of such restriction, use or disclose otherwise restricted health information to a health care provider to the extent the patient is in need of emergency treatment and such information is needed to provide the emergency treatment. However, if a member of VUOM's personnel discloses restricted health information to a health care provider for treatment, such VUOM personnel must request that the health care provider who receives the information not further use or disclose the information.
3. **Including a Restriction in the Patient's Medical Record:** If VUOM agrees to any request by a patient to restrict the uses and disclosures of his/her health information, details regarding such restriction must be placed prominently in the patient's medical record.
4. **Limitations on Restrictions:** Any restriction described in Section A.1 above which is agreed to by VUOM personnel is not effective to prevent uses and disclosures: (a) required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine Covered Entity's compliance with the HIPAA Privacy Standards; (b) permitted in connection Section 1 of Chapter 111.8 of this Manual (with respect to patient directories); and (c) permitted pursuant to Section D of Chapter III.A of this Manual (regarding uses and disclosures for which consent, individual authorization or the opportunity to agree or object is not required).



5. **Termination of Restriction by VUOM:** VUOM may terminate its agreement to any restriction if: (a) the patient agrees to or requests the termination in writing (b) the patient orally agrees to the termination and the oral agreement is documented; or (c) VUOM informs the patient that it is terminating its agreement to a restriction, except that such termination is only effective with respect to the health information created or received after VUOM has so informed the patient. To the extent VUOM agrees to a restriction, it must document the restriction in writing and maintain a copy in the patient record for a period of six (6) years from the date when it last was in effect.

### Requests by Patients to Receive Communications by Alternative Means or at Alternative Locations

1. **Permitting Patients to Request to Receive Communications by Alternative Means:** VUOM must permit patients to request and must accommodate reasonable requests by patients to receive communications regarding their health information by alternative means or at alternative locations.
2. **Required Form of Request:** Any such request by a patient must be in writing and describe the following: (a) specification of an alternative address or other method of contact, and (b) information on how payment, if any, will be handled, when appropriate. VUOM personnel are not permitted to require the patient to provide an explanation as to the basis for his/her request as a condition of providing communication on such confidential basis.
3. **Including a Patient's Request in the Patient's Medical Record:** If VUOM agrees to provide the patient communications by alternative means or at an alternative location, details regarding the alternative means or alternative location shall be placed prominently in the patient's medical record.

### Access of Patients To Their Health Information

Patients have certain basic rights with respect to their health information created or received by VUOM. For example, patients have the right of access to inspect and copy certain health information used by VUOM, in whole or in part, to make decisions about them. It is VUOM's policy that VUOM personnel afford patients this right by complying with the procedures set forth below.

### Patient Access Procedures

1. **Request by Patient:** Any request by a patient to inspect and/or copy his/her health information must be in writing and directed to VUOM's Privacy Officer.
2. **Time Limit for Providing/Denying Access:** In general, VUOM must act on a patient's request for access no later than thirty (30) days after receipt of the request. If VUOM grants the request, in whole or in part, it must inform the patient of the acceptance of the request and provide the access requested. If VUOM denies the request, in whole or in part, it must provide the patient with a written denial in accordance with Section 10 below. If the request for access is for health information that is not maintained or accessible by VUOM on-site, VUOM must take action by no later than sixty (60) days from the receipt of such request. If VUOM is unable to take the action required in such time, VUOM may extend the time for such action by no more than thirty (30) days provided: (a) VUOM, within the applicable time limit set forth above, provides the patient with a written statement of the reasons for the delay and the date by which VUOM will complete its action on the patient's request; and (b) VUOM may have only one such extension of time for action on a patient's request for access.
3. **Information a Patient Has the Right to Access:** In general, a patient has the right of access to inspect and copy health information used by VUOM, in whole or in part, to make decisions about the patient. This right, however, does not extend to certain types of information (see Section 4 below). In addition, VUOM may, under certain circumstances, deny a patient access to his or her health information regardless of whether such information is contained in the patient's records (see Section 5 below).
4. **Information a Patient Does Not Have the Right to Access:** A patient does not have the right to access the following: (a) psychotherapy notes; (b) information compiled in reasonable anticipation of, or



for use in, a civil, criminal or administrative action or proceeding; (c) information held by clinical laboratories if the Clinical Laboratory Improvements Amendments of 1988 ("CLIA") prohibits such access (i.e., the patient is not, under applicable law, an "authorized person" who is permitted to receive the laboratory test record or report); or (d) health information held by certain research laboratories that are exempt from the CLIA regulations.

5. **Grounds for Denial of Access.** VUOM may, under the circumstances listed below, deny a patient access to information he or she would otherwise be entitled to access. However, as set forth below, a patient may have the right to request that VUOM review its denial.

Page | 8

a. **Grounds for Denial That are Not Subject to Review:** VUOM may deny a patient's right to access his or her health information in the following circumstances:

- (i) **Information Excepted from the Right of Access:** VUOM may deny access to any information described in Section 4 above;
- (ii) **Request by Inmate of a Correctional Institution:** To the extent VUOM is acting under the direction of a correctional institution, VUOM may deny, in whole or in part, the request by an inmate to obtain a copy of his or her health information if providing such copy would jeopardize the health, safety, security, custody or rehabilitation of the inmate or other inmates or the safety of any officer, employee or other person at such institution or any person responsible for transporting the inmate;
- (iii) **Information Obtained in the Course of Research That Includes Treatment:** A patient's access to his or her information created or obtained by VUOM in the course of research that includes treatment may be temporarily suspended for as long as research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in such research and VUOM has informed the patient that his or her right of access will be reinstated upon completion of the research;
- (iv) **Information Subject to the Privacy Act:** A patient's access to his or her health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law; or
- (v) **Information Received from Non-Health Care Providers:** VUOM may deny access to information if VUOM obtained the information from someone other than a health care provider under a promise of confidentiality and the access requested would not be reasonably likely to reveal the source of the information.

b. **Grounds for Denial Subject to Review:** VUOM may deny a patient's right to access his or her health information in the following circumstances; however, the patient has the right to request that any such denial be reviewed:

- (i) **Endangerment of Patient:** A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;
- (ii) **Information Makes Reference to Others:** The patient health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or



- (iii) **Request by a Personal Representative:** The request for access is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.
6. **Providing the Access Requested:** If VUOM provides a patient with access, in whole or in part, to his or her health information, VUOM must provide the access requested by the patient including inspection or obtaining a copy (or both). If the same information that is the subject of a request for access is maintained in more than one record or at more than one location, VUOM need only produce the health information once in a response for request for access.
7. **Form of Access Requested:** VUOM must provide the patient with access to his or her information in the form or format requested by the patient, if it is readily producible in such form or format or, if not, in a readable hard copy form or such other form or format as agreed to by VUOM and the patient. VUOM may provide the patient with a summary of the information requested in lieu of providing access to the information or may provide an explanation of the information to which access has been provided if (a) the patient agrees in advance to such a summary or explanation, and (b) the patient agrees in advance to the fees imposed, if any, by VUOM for such summary or explanation.
8. **Time and Manner of Access:** VUOM must provide the access as requested by the patient in a timely manner, including arranging with the patient for a convenient time and place to inspect or obtain the copy of the health information, or mailing a copy of the information at the patient's request. VUOM may discuss the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely provision of access.
9. **Fees:** If the patient requests a copy of his or her health information or agrees to a summary or explanation of such information, VUOM may impose a reasonable, cost-based fee, provided that the fee includes only the cost of: (a) copying (including the cost of supplies for and labor of copying) the health information requested by the patient; (b) postage, when the patient has requested that a copy, a summary or explanation be mailed; and (c) preparing an explanation or summary of the health information, if agreed by the patient as required by Section 7 above.
10. **Denial of Access:** If VUOM denies access, in whole or in part, to health information, the Privacy Officer must provide a timely, written denial to the patient in accordance with Section 2 above. The denial must be in plain language and contain: (a) The basis for the denial; (b) If applicable, a statement of the patient's review rights under Section 13 of this section, including a description of how the patient may exercise such review rights; and (c) A description of how the patient may complain to VUOM (including the name, title and telephone number of the contact person or office) or to the Secretary of the Department of Health and Human Services pursuant to the complaint procedures described in Chapter IV of this Manual.
11. **Making Other Information Accessible:** VUOM must, to the extent possible, give the patient access to any other health information requested, after excluding the information as to which VUOM has a ground to deny access.
12. **Other Repository of Information:** If VUOM does not maintain the health information that is the subject of the patient's request for access and VUOM knows where the requested information is maintained, VUOM must inform the patient where to direct the request for access.
13. **Review Process:** If access is denied for a reason described in Section 5.b above, the patient has the right to have such denial reviewed by a licensed health care professional who is designated by VUOM to act as a reviewing official and who did not participate in the original decision to deny. VUOM must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in Section 5.b above. VUOM must promptly



provide written notice to the patient of the determination of the reviewing official and take such other action as required by law to carry out the reviewing official's determination.

14. **Documentation:** VUOM must document the following and retain such documentation for at least six (6) years from the date of their creation or the date when they last were in effect, whichever is later: (a) the records that are subject to access by patients; and (b) the titles of the persons or offices responsible for receiving and processing requests for access by patients. VUOM medical records are also covered by VUOM's record retention policy, which requires that VUOM medical records be retained for periods longer than six (6) years.

### Amending Health Information

Patients have certain rights with respect to their health information. For example, patients have the right to have Covered Entity amend their health information under certain circumstances as long as the health information is maintained by Covered Entity. It is the policy of Covered Entity that its personnel afford patients this right by complying with the procedures set forth below.

### Amendment Procedures

1. **Request by Patient:** Any request by a patient to have VUOM amend his/her health information must be in writing and directed to VUOM's Privacy Officer. Any such request must provide a reason to support the requested amendment.
2. **Process for Reviewing Patient's Request:** The Privacy Officer or the Privacy Officer's designee shall review the request upon receipt and consult with the health care provider(s) involved in the patient's care and the Privacy Committee to determine whether or not the requested amendment is appropriate. Any request for amendment should be honored except in those cases where VUOM should deny the patient's request as set forth in Section 5 below.
3. **Time Limit for Responding to Patient's Request:** Any request for amendment must be acted on no later than sixty (60) days after receipt. If VUOM the requested amendment, in whole or in part, it must take the actions described in Section 4 below. If VUOM denies the requested amendment, in whole or in part, it must provide the patient with a written denial in accordance with Section 4 below. If VUOM is unable to act on the amendment within such sixty (60) day period, VUOM may extend the time for such action by no more than thirty (30) days as long as VUOM, within the original sixty (60) day period, provides the patient with a written statement of the reasons for the delay and the date by which VUOM will complete its action on the patient's request. VUOM may only have one such extension of time for action on the request for amendment.
4. **Required Actions for Accepted Requests:** If VUOM accepts the requested amendment, in whole or in part, VUOM must take the following actions:
  - a. Make the appropriate amendment to the patient's health information or record that is the subject of the requested amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment;
  - b. Timely inform the patient that the amendment is accepted and obtain the patient's identification of and agreement to have VUOM notify the relevant persons with which the amendment needs to be shared; and
  - c. Make reasonable efforts to inform and provide the amendment within a reasonable time to (i) persons identified by the patient as having received health information about the patient and needing the amendment, and (ii) persons, including VUOM's Business Associates, that VUOM knows have the patient's health information that is the subject of the amendment and that may have relied on, or could foreseeable rely on, such information to the detriment of the patient.
5. **Denying Patient's Request:** The Privacy Officer or Privacy Officer's designee should deny the patient's request



for amendment if it is ultimately determined that the health information or record that is subject to the request:

- a. Was not created by VUOM (unless the patient provides a reasonable basis to believe that the originator of the disputed health information is no longer available to act on the requested amendment);
  - b. Is not part of the designated record set;
  - c. Would not be available for inspection by the patient (see Chapter II.C of this Manual relating to a patient's right to access his or her information); or
  - d. Is accurate and complete.
6. **Required Actions for Denied Requests:** If VUOM denies the requested amendment, in whole or in part, VUOM must take the following actions:
- a. Provide the patient with a timely written denial as required in Section 3 above. The denial must use plain language and contain:
    - (i) The basis for the denial;
    - (ii) The patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;
    - (iii) A provision saying that, if the patient does not submit a statement of disagreement, the patient may request that VUOM provide the patient's request for amendment and the denial with any future disclosures of patient health information that is the subject of the amendment; and
    - (iv) A description of how the patient may complain to VUOM or to the Secretary of the Department of Health and Human Services pursuant to the complaint procedures described in Chapter IV of this Manual.
  - b. VUOM must also permit the patient to submit a written statement disagreeing with the denial of all part of the requested amendment and the basis for such disagreement. VUOM may reasonably limit the length of the statement of disagreement.
  - c. VUOM may prepare a written rebuttal to the patient's statement of disagreement. If VUOM prepares such a rebuttal, VUOM must provide a copy to the patient.
  - d. VUOM must, as appropriate, identify the record or health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient's request for an amendment, VUOM 's denial of the request, the patient's statement of disagreement, if any, and VUOM 's rebuttal, if any, to the designated record set.
  - e. With respect to any future disclosures, VUOM must comply with the following requirements:
    - (i) If a statement of disagreement has been submitted by the patient, VUOM must include the material appended in accordance with Section 6.d. above. Alternatively, VUOM may include an accurate summary of such information, with any subsequent disclosure of the health information to which the disagreement relates;
    - (ii) If the patient has not submitted a written statement of disagreement, VUOM must include the patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the health information only if the patient has requested such action in accordance with Section 6.a.iii. above.



- (iii) When the subsequent disclosure described in Section 6.e.i. or 6.e.ii. above is made during a standard HIPAA transaction that does not permit the additional material to be included with the disclosure, VUOM may separately transmit the material required by Section 6.e.i. or 6.e.ii., as applicable, to the recipient of the standard HIPAA transaction.
- f. If VUOM receives or is informed by another health care provider, health care clearinghouse or health care plan of an amendment to a patient's health information, VUOM must amend the health information in designated record sets as provided in Section 4.a. of this section.
7. **Documentation:** VUOM must document the titles of the persons or offices responsible for receiving and processing requests for amendments by patients and retain the documentation for at least six (6) years from the date of its creation. VUOM's medical records, including any amendments of such medical records are also covered by VUOM's record retention policy, which requires that VUOM's medical records be retained for periods longer than six (6) years. Please consult the record retention policy for the appropriate retention period.

### Accounting of Disclosures

Patients have certain rights with respect to their health information. For example, patients have the right to receive, subject to certain exceptions, an accounting of the disclosures of their health information made by Covered Entity in the six (6) years prior to the date on which the accounting is requested. It is the policy of Covered Entity that

Covered Entity personnel afford patients such right by complying with the procedures set forth below.

### Procedures for Accounting of Disclosures

1. **Request by Patient of an Accounting of Disclosures:** Any requests by a patient to receive an accounting of disclosures of his/her health information must be in writing and submitted to the Privacy Officer or Privacy Officer's designee at the respective clinic locations as shown on Page 8.
2. **Time Limits on Responding to Patient's Request:** VUOM must provide the patient with the requested accounting no later than sixty (60) days following the receipt of such request. If VUOM is unable to provide an accounting within such sixty (60) day period, VUOM may extend the time to provide the accounting by no more than thirty (30) days as long as VUOM, within the original sixty (60) day period, provides the patient with a written statement of the reasons for the delay and the date by which VUOM will provide the accounting. VUOM may have only one thirty (30) day extension of time for action on any request for an accounting.
3. **Fees:** VUOM must provide the first accounting to a patient in any twelve (12) month period without a charge. VUOM may, however, impose a reasonable cost based fee for each subsequent request by the same patient within such twelve (12) month period as long as VUOM informs the patient in advance of the fee to be charged by VUOM and provides the patient with an opportunity to withdraw or modify his/her request in order to avoid or reduce such fee.
4. **Information Required to be Included in Accounting: Limitations:** VUOM must provide the patient with an accounting of disclosures of patient's health information made by VUOM and VUOM's Business Associates during the six (6) years prior to the date on which the accounting is requested, except for disclosures:
  - a. To carry out treatment, payment and health care operations;
  - b. To the patient;
  - c. Incident to a permitted use or disclosure;
  - d. Pursuant to an authorization;



- e. For VUOM 's patient directory purposes;
  - f. To persons involved in the patient's care or for other notification purposes;
  - g. For national security or intelligence purposes;
  - h. To correctional institutions or law enforcement officials;
  - i. As part of a limited data set (partially de-identified information that used for specific purposes);
  - j. That occurred prior to April 14, 2003 (the compliance date of the HIPAA Privacy Standards).
5. **Suspending Patient's Right to Receive an Accounting:** VUOM must temporarily suspend a patient's right to receive an accounting of disclosures made by VUOM to a health oversight agency or law enforcement official (as described in Section C of Chapter III.A. of this Manual), for the time specified by such agency or official, if such agency officially provides VUOM with a written statement that such an accounting to the patient would be reasonably likely to impede the agency's activities and specifying the time which such suspension is required. However, if the agency or official statement is made orally, VUOM must (a) document the statement, including the identity of the agency or official making the statement; (b) temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and (c) limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement described above is submitted during that time.
6. **Information Required to Be Included in Accounting:** The written accounting provided by VUOM must meet the following requirements:
- a. Except for the excluded disclosures described in Section 5 above, the accounting must include disclosures of the patient's health information that occurred during the six (6) years prior to the date of the request (or such shorter time period as requested by the patient), including disclosures to or by VUOM 's Business Associates;
  - b. The accounting must include the following for each disclosure listed: (i) the date of the disclosure, (ii) the name of the entity or person who received the health information and, if known, the address of such entity or person, (iii) a brief description of the health information disclosed, and (iv) a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure (or, in lieu of such statement, a copy of a written request for disclosure made by the Secretary of the U.S. Department of Health and Human Services or under one of the other regulatory exceptions, if any).
  - c. If during the period covered by the accounting, VUOM has made multiple disclosures of the patient's health information to the same person or entity for a single purpose under one of the regulatory exceptions or to the Secretary of the U.S. Department of Health and Human Services, the accounting may, with respect to such multiple disclosures, provide (i) the information described in Section 6.b. above for the first disclosure during the accounting period; (ii) the frequency, periodicity or number of the disclosures made during the accounting period; and (iii) the date of the last such disclosure during the accounting period.
7. **Disclosure for Research:** VUOM has other accounting requirements for disclosures of patient health information for particular research purposes.
8. **Documentation Requirements:** VUOM must document the following and retain documentation for six (6) years from the date of its creation or the date when it last was in effect:
- a. The information described in Section 6 above for disclosures of health information that are subject to an accounting under Section 5 above;



- b. The written accounting that is provided to the patient; and
- c. The titles of the persons or offices responsible for receiving and processing requests for an accounting by patients.

## USING, DISCLOSING AND REQUESTING PROTECTED HEALTH INFORMATION

### Permitted Uses and Disclosures of Patient Health Information without Patient Consent or Authorization

VUOM is permitted to use and disclose a patient's health information without obtaining the patient's consent or authorization for the purposes set forth below. This policy outlines the procedures VUOM personnel must follow when using or disclosing patient health information for such purposes.

#### Permitted Uses and Disclosures

- For VUOM's own treatment, payment or health care operations.
- Required by law.
- Public health activities.
- Health oversight activities.
- Information regarding decedents.
- Cadaveric organ, eye or tissue donation purposes.
- Research.
- To avert serious threat to health or safety.
- Specialized government functions

#### Permitted Disclosures

- Subject to certain limitations, disclosures for the treatment, payment or health care operations of a third party.
- Victims of abuse, neglect or domestic violence.
- Judicial and administrative proceedings.
- Law enforcement purposes.
- Workers' compensation.

### Procedures for Permitted Uses & Disclosures of Patient Health Information Without Patient Authorization

- A. **Application:** The following procedures generally do not apply to the use or disclosure of psychotherapy notes or patient health information for the purpose of marketing. Both topics are addressed in more detail in the policy contained in Chapter III.C entitled "Permitted Uses and Disclosures of Patient Health Information Pursuant to a Patient's Authorization."
- B. **Use and Disclosure of Patient Health Information**
  1. Use of Patient Health Information by VUOM's Personnel: VUOM personnel and assigned student interns are permitted, without obtaining the patient's consent or authorization, to use patient health information for purposes of VUOM's treatment, payment and health care operations. In addition, VUOM personnel and assigned student interns are permitted, under certain circumstances, to use patient health information for the treatment, payment and health care operations of third parties. In general, clinical personnel who are involved in patient care are entitled to access and use the entire medical record of the patients they are treating on a need-to-know basis. Clinical personnel or student interns, however, may not access or use the medical record of a patient, unless they are treating, or assisting another in treating, such patient. In addition, before using a patient's health information, VUOM personnel and student interns should comply with any restriction on the use of a patient's health information agreed to by VUOM pursuant to Chapter 11.8 of this Manual. Non-clinical personnel are permitted to access and use the health information of VUOM patients for purposes of treating the patient, obtaining payment for services provided to the patient or VUOM's



health care operations. However, VUOM personnel may only access and use the minimum amount of health information necessary to carry out their duties. In addition, regardless of whether a use exception applies, VUOM personnel are prohibited from using any patient health information in violation of a restriction on the use of a patient's health information agreed to by VUOM pursuant to Chapter II.B of this Manual. The Privacy Officer has established various classes of VUOM personnel who need access to patient health information to perform their duties, the categories of patient health information to which access is needed, and the conditions appropriate to such access. It is the responsibility of each member of VUOM's workforce to understand the patient health information they are permitted to access and use to perform their duties. If you have any questions about the types of patient health information you are permitted to access and use to perform your duties, ask your supervisor or contact the Privacy Officer. The following outline various examples of appropriate and inappropriate uses of patient health information by VUOM personnel:

#### Examples of appropriate uses of patient health information

- (i) Health care professional (e.g., Faculty Clinician, assigned Student Intern etc.) using patient health information for the purposes of rendering care to a patient.
- (ii) Billing personnel accessing and using the patient health information necessary for billing for services rendered.
- (iii) VUOM administrative personnel using the patient health information that is necessary to prepare a financial analysis to assess the business impact of patient care.

#### Examples of inappropriate uses of patient health information

- (i) Health care professional or students accessing or using the health information of patients they are not treating or assisting others in treating.
  - (ii) Accessing/using medical records or VUOM's computer system to determine whether an individual (e.g., coworker, relative, celebrity, etc.) is receiving treatment and there is no legitimate reason to have such knowledge.
  - (iii) Using the medical record of a member of VUOM's personnel to verify they were really sick, had a workers' compensation injury, etc.
2. Disclosing Patient Health Information to Third Parties: VUOM personnel are permitted to disclose a patient's health information to a third party without first obtaining the patient's consent or authorization to the extent such disclosure is permitted by law. To assist VUOM personnel in determining the types of disclosures permitted, the Privacy Officer has established standard protocols for various disclosures that are made by VUOM on a routine and recurring basis. These protocols are described in VUOM's [Standard Protocols for Disclosing and Requesting Patient Health Information](#) and outline the requirements relating to many routine disclosures (e.g., whether the disclosure is subject to the minimum necessary standard, how VUOM personnel should comply with the minimum necessary standard, if applicable, etc.). To the extent a standard protocol has not been established for a particular disclosure (or if a member of VUOM's personnel is not sure whether a particular protocol applies in a given situation), VUOM personnel should obtain approval from the Privacy Officer or his or her designee before making the disclosure. In addition, regardless of whether a disclosure exception applies, VUOM personnel and students are prohibited from disclosing any patient health information in violation of a restriction on the use of a patient's health information agreed to by VUOM pursuant to Chapter 11.8 of this Manual. Furthermore, VUOM may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when (1) making disclosures to public officials that are described in Section D below, if the public official represents that the information requested is the minimum necessary for the state purposes; (2) the information is requested by a health plan, health care clearinghouse or HIPAA covered health care provider; (3) the information is requested



by a professional who is a member of VUOM 's workforce or is a business associate of VUOM for the purpose of providing professional services to VUOM; or (4) certain documentation or representations have been provided by a person requesting the information for research purposes.

**Use and Disclosure for Purposes of Treatment, Payment and Health Care Operations**

1. **Treatment:** Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
  
2. **Payment:** Payment includes those activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under a health plan. Payment also includes the activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care. Such activities relate to an individual to whom health care is provided and include, but are not limited to the following:
  - a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
  - b. Risk adjusting amounts based on enrollee health status and demographic characteristics;
  - c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
  - d. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
  - e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
  - f. Disclosure to consumer reporting agencies of any of the following patient health information relating to collection of reimbursement: (i) name and address; (ii) date of birth; (iii) social security number; (iv) payment history; (v) account number; and (vi) name and address of the health care provider and/or health plan.
  
3. **Health Care Operations:** Health care operations include any of the following activities of the covered entity to the extent that the activities are related to covered functions:
  - a. **Quality Assessment and Improvement:** Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
  - b. **Reviews and Evaluations:** Reviewing the competence or qualifications of health care professionals, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;



- c. **Contract Placement:** Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
- d. **Professional Services:** Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- e. **Business Planning:** Business planning and development, such as conducting cost-management and planning-related analyses relating to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies;
- f. **Business Management and Administration:** Business management and general administrative activities of the entity, including, but not limited to, the following: (i) management activities relating to implementation of and compliance with HIPAA requirements; (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that patient health information is not disclosed to such policy holder, plan sponsor, or customer; (iii) resolution of internal grievances; (iv) the sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) consistent with the applicable requirements of the Privacy Standards, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

#### Other Regulatory Exceptions Regarding Use and/or Disclosure

This section outlines the regulatory exceptions pursuant to which VUOM personnel are permitted to disclose and/or use patient health information without the consent or authorization of the patient. The following is a general summary of the regulatory exceptions set forth in 45 C.F.R. § 164.512; it does not describe the specific requirements for each exception. The Privacy Officer may consider incorporating the specific requirements for relevant exceptions in this policy or attaching the specific requirements as a supplement to this policy.

1. **Required by Law:** When it is required by law and the use or disclosure is limited to the relevant requirements of such law;
2. **Public Health Activities:** When it involves use and disclosure for public health activities, such as mandated disease reporting, the reporting of vital events, births, deaths, etc.;
3. **Health Oversight Activities:** When disclosing information for the purpose of health oversight activities, such as audits, investigations, licensure or disciplinary actions or legal proceedings or actions;
4. **Information Regarding Decedents:** When disclosing information about deceased persons to medical examiners, coroners and funeral directors;
5. **Organ Donation:** When disclosing or using information for organ and tissue donation purposes;
6. **Research:** When disclosing information related to a research project when a waiver of authorization has been approved by the Institutional Review Board;
7. **Health or Safety Threat:** When the Privacy Officer believes in good faith that the disclosure is necessary to avert a serious health or safety threat to the patient or to the public's safety;
8. **Military Activity and National Security:** When disclosure is necessary for specialized government functions, such as military service, for the protection of the president or for national security and intelligence activities.



## Disclosure

1. **Abuse or Neglect:** When reporting information about victims of abuse, neglect or domestic violence as required by law;
2. **Legal Proceedings:** When disclosing information for judicial and administrative proceedings in accordance with state and/or federal law; for instance, in response to a court order, such as a subpoena or discovery request.
3. **Law Enforcement:** When disclosing information for law enforcement purposes, for instance, to locate or identify a suspect, fugitive, witness or missing person, or regarding a victim of a crime who can not give consent or authorization because of incapacity;
4. **Workers' Compensation:** When disclosure is necessary to comply with workers' compensation laws or purposes;
5. **Inmates:** In the case of a prison inmate, information can be released to the correctional facility in which he or she resides for the following purposes: (a) for the institution to provide the inmate with health care; (b) to protect the health and safety of the inmate or the health and safety of others; or (c) for the safety and security of the correctional facility.

VUOM is permitted, in certain circumstances, to use or disclose certain patient health information without the patient's written consent or authorization provided that the patient is informed in advance of the use or disclosure and has had the opportunity to agree to, prohibit or restrict the use or disclosure of such information. This policy describes the circumstances when such uses and disclosures are permitted and the procedures VUOM personnel must follow to order to comply with applicable laws.

### Procedures to Use or Disclose Patient Health Information Without Patient's Consent

1. **Patient Directory:** Unless an objection is expressed, VUOM may include *the* patient's name, location in VUOM, general medical condition, and religious affiliation (for purposes of informing clergy) in VUOM's Patient Directory. Any of this information may be disclosed to members of the clergy. Any of this information, except for religious affiliation, may be disclosed to other persons who ask for the patient by name. The patient will be informed in VUOM's Notice of Privacy Practices of the information to be included in VUOM's Patient Directory and the persons to whom VUOM may disclose such information, as well as provided with the opportunity to restrict or prohibit some or all of the uses and disclosures. In the event of the patient's incapacity or an emergency treatment circumstance, where the opportunity to object cannot practicably be provided, VUOM may include the above-described information in VUOM's Patient Directory and disclose in the limited manner described so long as (a) consistent with any prior expressed preference of the patient known to VUOM and (b) determined by VUOM, in the exercise of professional judgment, to be in the patient's best interest.
2. **Others Involved in Patient's Care:** VUOM may disclose to a family member, other relative or a close personal friend of the patient, or any other person identified by the patient, health information directly relevant to such person's involvement with the patient's care or payment related to the patient's health care. VUOM may also use or disclose health information to notify, or assist in the notification of (including identifying or locating) a family member, a personal representative of the patient, or another person responsible for the care of the patient's location, general condition or death. VUOM personnel are permitted to orally inform the patient of, and obtain the patient's oral agreement or objection to, the use or disclosure.

Before releasing information to a person covered by this category, VUOM must either

- a. obtain the patient's agreement; or



- b. provide the patient with the opportunity to object to the disclosure, and the patient does not do so; or
- c. Reasonably infer from the circumstances, based on the exercise of professional judgment that the patient does not object to the disclosure.

Examples of situations in which VUOM can "reasonably infer from the circumstances" that the patient does not object to the disclosure include: Page | 19

- a. When a spouse is present when treatment is being discussed with the patient; and
  - b. When a colleague or friend has brought the patient to VUOM's for treatment and the patient has invited them into the exam/treatment room. If the patient is not present (or cannot agree or object to the use or disclosure of his or her health information because he or she is unconscious or incapacitated) or it is an emergency, then VUOM may exercise professional judgment to determine whether disclosure is in the best interest of the patient, and then may disclose only the health information that is directly relevant to the person's involvement with the patient's health care.
3. Disaster Relief Agencies: VUOM may use or disclose health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the notification of family and friends regarding the patient's location, general condition or death. VUOM should attempt to obtain the patient's agreement to such use or disclosure to the extent that VUOM, in the exercise of professional judgment, determines that obtaining such agreement does not interfere with the ability to respond to the emergency circumstances.
  4. Fundraising Activities: For the purpose of raising funds for its own benefit, VUOM may use internally, or disclose to a Business Associate or to an institutionally related foundation, the following: (a) demographic information relating to a patient, including name, address and other contact information, age, gender and insurance status, and (b) dates of service. Any fundraising materials sent to a patient must contain a description of how the patient may opt out of receiving any further fundraising communications in the future.

It is the policy of VUOM that VUOM personnel not use or disclose a patient's health information without the patient's written authorization unless VUOM is otherwise permitted or required to make such use or disclosure. This policy outlines authorization requirements and sets forth the required procedures VUOM personnel must follow when the patient's authorization is required. For situations in which VUOM is permitted or required to use and disclose a patient's health information without the patient's consent or authorization, see Chapter III.A of this Manual. For situations in which VUOM is permitted to use and disclose a patient's health information so long as the patient is first given an opportunity to agree to, prohibit or object, see Chapter III.B of this Manual.

## Procedures When the Patient's Authorization is Required

### Authorization in General

1. **Authorization Requirements:** In general, a valid authorization must contain the following core elements: (a) a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion; (b) the identification of the persons or class or persons authorized to make the use or disclosure; (c) the name or other specific identification of the persons or class of persons to whom VUOM may make the use or disclosure; (d) a description of each purpose of the use or disclosure; (e) an expiration date or event; (e) the signature of the patient (or the patient's personal representative) and date; and (f) if signed by a personal representative, a description of such person's authority to act on behalf of the patient.

A valid authorization must also (a) be written in plain language; (b) contain specific statements regarding the patient's right to revoke the authorization and the ability or inability of VUOM to



condition treatment, payment, enrollment or eligibility for benefits on the authorization; and (c) contain a statement adequate to place the patient on notice of the potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected.

2. **Prohibition on Conditioning of Authorizations:** VUOM may not condition the provision to an individual of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except:
- (i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of health information for such research (see Section B.2.
  - (ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if (a) the authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and (b) the authorization is not for a use or disclosure of psychotherapy notes.
  - (iii) A health plan, health care clearinghouse or HIPAA covered health care provider may condition the provision of health care that is solely for the purpose of creating health information for disclosure to a third party on provision of an authorization for the disclosure of the patient health information to such third party (e.g., VUOM is performing preemployment drug testing or fitness-for-duty exams, etc.).
3. **Prohibition on Combining Authorizations:** Authorizations may not be combined with any other document to create a compound authorization, except as follows:
- (i) Combined authorizations are permitted in connection with certain research activities (see Section B.1. below).
  - (ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes (see Section B.2. below).
  - (iii) An authorization (other than one for a use or disclosure of psychotherapy notes) may be combined with any other authorization, except when VUOM has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations (see Section A.2. above).
4. **Processing Requests of Patient Health Information Pursuant to an Authorization Received from a Third Party:** All requests for release of health information pursuant to written patient authorization shall be referred to the VUOM Privacy Officer. Before releasing any information regarding the patient to the requestor, VUOM personnel should (a) verify that the authorization contains the entire core elements described above, and (b) verify the identity of the requestor in accordance with Chapter 111.0 of this Manual.
5. **Authorizations Requested by VUOM Copy to Patient:** If VUOM personnel request a patient to sign an authorization, the patient must be provided with a copy of the signed authorization. The Privacy Officer will establish standard protocols in which VUOM personnel will be permitted to request a patient to execute an authorization. However, to the extent no standard protocol has been established, VUOM personnel must obtain the approval of the Privacy Officer before asking a patient to execute an authorization. VUOM's standard Authorization for the Use and Disclosure of Patient Health Information is included in Appendix B to this Manual.



- 6. **Limits on Using or Disclosing Information Pursuant to an Authorization:** Any use or disclosure made by VUAOM personnel pursuant to an authorization must be consistent with the authorization (i.e., made while the authorization is effective, limited to the purpose(s) of the authorization, etc.).
  
- 7. **Revocation of Authorizations:** A patient may revoke his/her authorization at any time by notifying the Medical Records Department in writing except to the extent that:
  - (i) VUOM has taken action in reliance thereon; or
  - (ii) The authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself. VUOM's standard Revocation of Authorization Form, a copy of which is included in Appendix B to this Manual, should be provided to the patient upon request. The revocation must be kept with the original authorization form and a copy must be given to the patient.
  
- 8. **Transition Provisions:** Except for certain prior permissions for research which are subject to different requirements (see Section B.1. below), VUOM may use or disclose protected health information that it created or received prior to April 14, 2003 (the compliance date of the HIPAA Privacy Standards), pursuant to an authorization or other express legal permission obtained from the patient prior to April 14, 2003, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction as described in Section A.1. of Chapter II.B. of this Manual.

**Special Requirements for Certain Activities**

- 1. **Research:** [Note; The research provisions described below do not encompass all requirements relating to research activities.
  - a. **General:** In general, VUOM is permitted to use or disclose a patient's health information for research purposes (as defined below) only with a patient's written authorization, except in the following three situations:
    - (i) When an Institutional Review Board (IRB) or Privacy Board has approved a waiver of authorization;
    - (ii) The use or disclosure is sought solely to review patient health information as necessary to prepare a research protocol or for similar purposes preparatory to research; or
    - (iii) The use or disclosure is sought solely for research on the health information of decedents.
  
  - b. **Definition.** "Research" is defined as a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Note that studies relating to quality assessment and improvement activities may qualify as "health care operations" and may be used and disclosed without obtaining the patient's authorization (see Chapter III.A of this Manual).
  
  - c. **Permitted Use of Compound Authorizations:** An authorization for the use or disclosure of patient health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of patient health information for such research or a consent to participate in such research.
  
  - d. **Criteria for Waiver of Authorization:** An IRB or Privacy Board is authorized to approve a waiver of authorization if the following criteria are met:



- (i) The use or disclosure of patient health information involves no more than a minimal risk to the privacy of patients, based on, at least, the presence of the following elements:
  - 1. An adequate plan to protect the identifiers from improper use or disclosure;
  - 2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
  - 3. Adequate written assurances that the patient health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of patient health information would be permitted;
- (ii) The research could not practicably be conducted without the waiver or alteration; and
- (iii) The research could not practicably be conducted without access to and use of the patient health information.

e. **Transition Provisions:** VUOM may, to the extent allowed by one of the following permissions, use or disclose, for research, health information that it created or received either before or after April 14, 2003 (the applicable compliance date of the HIPAA Privacy Standards), provided that there is no agreed-to restriction as described in Section A.1. of Chapter II.B. of this Manual, and VUOM has obtained, prior to April 14, 2003, either:

- (i) An authorization or other express legal permission from an individual to use or disclose health information for the research; or
- (ii) The informed consent of the individual to participate in the research; or
- (iii) A waiver by an IRB of informed consent for the research, in accordance with applicable law, provided that VUOM must obtain authorization in accordance with Section A.1 above if, after April 14, 2003, informed consent is sought from an individual participating in the research.

**2. Psychotherapy Notes:**

a. General: VUOM must obtain a patient's written authorization meeting the requirements of Section A.1 above for any use or disclosure of psychotherapy notes except in the following situations:

- (i) To carry out the following treatment, payment, or health care operations:
  - 1. Use by originator of the psychotherapy notes for treatment;
  - 2. Use or disclosure by VUOM for its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or



- 3. Use or disclosure by VUOM to defend a legal action or other proceeding brought by the patient; and
- (ii) When the use or disclosure is:
  - 1. Required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine Covered Entity's compliance with the HIPAA Privacy Standards;
  - 2. Required by law;
  - 3. Made to a health oversight agency with respect to the oversight of the originator of the psychotherapy notes;
  - 4. Made to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; or
  - 5. Made to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, or as required by law.
- b. **Definition:** "Psychotherapy notes" are defined as notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. The term psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

**3. Marketing**

- a. General: VUOM must obtain an authorization for any use or disclosure of health information for marketing, except if the communication is in the form of:
  - (i) A face-to-face communication made by VUOM to a patient; or
  - (ii) A promotional gift of nominal value provided by VUOM.
- b. Marketing Activities: The term "marketing" means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:
  - (i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, VUOM who is making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits;
  - (ii) For treatment of that patient; or
  - (iii) For case management or care coordination for that patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of



care to that patient. The term "marketing" also includes an arrangement between VUOM and any other entity whereby VUOM discloses patient health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

- c. **Additional Authorization Requirements:** If the marketing involves direct or indirect remuneration to VUOM from a third party, the authorization must state that such remuneration is involved. Patients have certain basic rights with respect to their health information created or received by VUOM. Certain laws create a duty on the part of VUOM to verify, in certain circumstances, the identity of a person requesting health information from VUOM and the authority of any such person to have access to health information. It is VUOM policy that VUOM personnel afford patients this right by complying with the procedures set forth below.

## Procedures

- 1. Verify Identity and Authority:** Except with respect to uses and disclosures of health information in which the patient has the opportunity to object (see Chapter III.B of this Manual), VUOM personnel must verify the identity of a person requesting health information and the authority of any such person to have access to health information, if the identity or any such authority of such person is not known to VUOM. Routine communications between providers, where existing relationships have been established, do not require special verification procedures.
- 2. Documentation. Statements or Representations:** VUOM will also obtain any documentation, statements or representations, whether oral or written, from the person requesting the health information when such documentation, statement, or representation is a condition of the disclosure as described in Chapters III.A, III.B and III.C of this Manual. VUOM is entitled to rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements. For example, the conditions in the "Legal Proceedings" category in Section C.2. of Chapter III.A of this Manual (Permitted Uses and Disclosures of Health Information Without Patient Consent or authorization) may be satisfied by the administrative or judicial subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.
- 3. Identity of Public Officials:** VUOM may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of health information is to a public official or a person acting on behalf of the public official: a. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; b. If the request is made in writing, the request is on appropriate government letterhead; or c. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency (e.g., contract for services, memorandum of understanding, purchase order, etc.) that establishes that the person is acting on behalf of the public official.
- 4. Authority of Public Officials:** VUOM may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of health information is to a public official or a person acting on behalf of the public official: a. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; b. If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.



5. **Exercise of Professional Judgment:** The verification requirements are met if VUOM relies on the exercise of professional judgment in making a use or disclosure in those circumstances in which a patient has the opportunity to object (see Chapter 111.8 of this Manual) or acts on a good faith belief in making a disclosure in the "Health or Safety Threat" category under Section C. of Chapter III.A of this Manual.
6. **Privacy Officer:** If you have any questions regarding these verification procedures, please contact the Privacy Officer at the respective clinic locations as shown on Page 8. VUOM is required under certain circumstances to disclose a patient's health information to a third party.

It is VUOM's policy that VUOM disclose such information appropriately by complying with the procedures set forth below.

### Procedures

1. **Access of Patients to Their Health Information:** A patient generally has a right to inspect and copy the health information used by VUOM, in whole or in part, to make decisions about the patient. To the extent a patient has this right, VUOM is required to disclose such information to the patient. For specific information regarding the policies and procedures regarding patient access to health information, VUOM's personnel should review the policy, Access of Patients to Their Health Information, contained in Chapter II.C.
2. **Accounting of Disclosures:** A patient generally has a right to receive an accounting of certain disclosures of protected health information made by VUOM. To the extent a patient has this right, VUOM is required to disclose such information to the patient. For specific information regarding the policies and procedures regarding a patient's right to receive an account of disclosures, VUOM's personnel should review the policy, Accounting of Disclosures, contained in Chapter II.E.
3. **Request by HHS:** VUOM is required to disclose patient health information at the request of the Secretary of the U.S. Department of Health and Human Services in order to determine VUOM's compliance with the HIPAA Privacy Standards. If a member of VUOM's personnel receives such a request, he or she should immediately contact VUOM's Privacy Officer. Any disclosures made pursuant to this section should only be made by or under the direction of the Privacy Officer.
4. **Disclosures Required by Federal or State Law:** VUOM is required to disclose patient health information to the extent disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law. According to the HIPAA Privacy Standards, the term "required by law" means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. Any disclosures made pursuant to this section should only be made by or under the direction of the Privacy Officer.
5. **Privacy Officer:** If you have any questions regarding required disclosures, please contact the Privacy Officer. To the extent VUOM requests patient health information from a health plan, health care clearinghouse or health care provider, VUOM must, under certain circumstances, limit the amount of information requested. This policy outlines the procedures VUOM personnel must follow when requesting patient health information from a health plan, health care clearinghouse or health care provider. [Note: HIPAA's Minimum Necessary Standard requires that Covered Entity, under many circumstances, make certain efforts to limit the patient health information requested to the minimum amount necessary to accomplish the intended purpose of the request (see Chapter V.C. of



the Privacy Officer's Supplement for additional information regarding the Minimum Necessary Standard). The Privacy Officer should consider whether to include further discussion of the Minimum Necessary Standard in this policy or whether to merely incorporate limitations on requesting patient health information in the Standard Protocols for Disclosing and Requesting Patient Health Information, attached as Exhibit E to this Manual.

**Procedures**

1. **Limiting Information Requests:** Except as set forth in Section 2 below, when requesting patient health information from a health plan, health care clearinghouse or health care provider, VUOM personnel should limit the amount of information requested to the minimum amount necessary for the intended purpose of the request. To assist VUOM personnel in making such determination, the Privacy Officer has established standard protocols for various requests of patient health information made by VUOM on a routine and recurring basis. These standard protocols are set forth in VUOM's Standard Protocols for Disclosing and Requesting Patient Health Information (see Appendix E to this Manual) and outline the requirements relating to many routine requests (e.g., how VUOM personnel should comply with the minimum necessary standard, if applicable, etc.). To the extent a standard protocol has not been established for a particular request (or if a member of VUOM's personnel is not sure whether a particular protocol applies in a given situation), VUOM personnel should obtain approval from the Privacy Officer before requesting the information from a health plan, health care clearinghouse or health care provider.
2. **Requests by a Health Care Provider for Treatment:** The minimum necessary standard relating to requests for information do not apply to requests by a health care provider for treatment.
3. **Privacy Officer:** If you have any questions regarding required disclosures, please contact the Privacy Officer at [clinic@vuom.org](mailto:clinic@vuom.org).

**WORKPLACE TRAINING AND SANCTIONS FOR FAILURE TO COMPLY WITH POLICY AND PROCEDURES**

VUOM is required to train all members of its workforce, including certain non-employees and volunteers, on VUOM's policies and procedures with respect to the privacy of patient health information, as necessary and appropriate for the members of the workforce to carry out their function within VUOM. It is VUOM's policy to train all members of its workforce as described in the procedure set forth below.

**Procedures**

1. **Employees:** The following rules apply to the training of employees and sanctions for failure to comply with VUOM's policies with respect to the privacy of patient health information.
  - a. The Privacy Officer is responsible for scheduling training sessions for all existing VUOM employees prior to April 14, 2003. Employees will be trained as to VUOM's Policies and Procedures related to patient privacy.
  - b. New Employee Orientation programs will contain information regarding VUOM's Policies and Procedures related to patient privacy.
  - c. Documentation that an employee has received information and initial training about VUOM's Policies and Procedures must be placed in the employee's personnel file.
  - d. Any modifications or additions to VUOM's Policies and Procedures related patient privacy will be presented to all employees through utilization of employee in-services, memoranda or other appropriate methods within thirty (30) days of the modification or addition.
  - e. Documentation that an employee has received information and/or training about modifications or additions to VUOM's Policies and Procedures related to patient privacy



must be placed in the employee's personnel file.

- f. Employees will participate in reviews or updates of VUOM's Policies and Procedures related to patient privacy on a periodic basis as determined necessary and appropriate by the Privacy Officer in consultation with the Privacy Committee. Such reviews or updates may be conducted in conjunction with training related to modifications or additions to the existing Policies and Procedures.
- g. Documentation that an employee has attended a review or update session related to VUOM's Policies and Procedures related to patient privacy must be placed in the employee's personnel file.
- h. Employees who violate Policies and Procedures related to patient privacy will be subject to disciplinary action, up to and including termination.

2. **Non-employees and Volunteers:** The following rules apply to the training of non-employees and volunteers and sanctions for failure to comply with VUOM's policies with respect to the privacy of patient health information.

- a. The Privacy Officer is responsible for scheduling training sessions for all existing VUOM non-employees (i.e. medical staff, or others with VUOM privileges) and volunteers prior to April 14, 2003. These individuals will be trained as to VUOM's Policies and Procedures related to patient privacy.
- b. Orientation programs will contain information regarding VUOM's Policies and Procedures related to patient privacy. Non-employees and volunteers shall be required to complete Orientation programs prior to obtaining access to patient information.
- c. Documentation that a non-employee or volunteer has received information and initial training about VUOM's Policies and Procedures must be kept in a special section of VUOM's personnel files.
- d. Any modifications or additions to VUOM's Policies and Procedures related to patient privacy will be presented to all non-employees and volunteers through utilization of in-services, memoranda, or other appropriate methods within thirty (30) days of the modification or addition.
- e. Documentation that a non-employee or volunteer has received information and/or training about modifications or additions to VUOM's Policies and Procedures related to patient privacy must be placed and kept in a special section of VUOM's personnel files.
- f. Non-employees and volunteers will partake in reviews or updates of VUOM's Policies and Procedures related to patient privacy on a periodic basis as determined necessary and appropriate by the Privacy Officer in consultation with the Privacy Committee. Such reviews or updates may be conducted in conjunction with training related to modifications or additions to the existing policies and procedures.
- g. Documentation that a non-employee or volunteer has attended a review session related to VUOM's Policies and Procedures related to patient privacy must be placed in or kept in a special section of VUOM's personnel files.
- h. Non-employees who violate Policies and Procedures related to patient privacy will be subject to disciplinary action in accordance with VUOM's Policies and Procedures, up to and including revocation of any privileges in VUOM.



- i. Volunteers who violate Policies and Procedures related to patient privacy will be required to surrender their volunteer status at VUOM.

VUOM shares patient health information with certain other individuals and entities who provide services for or on behalf of VUOM ("Business Associates"). According to the HIPAA Privacy Standards, VUOM may disclose patient health information to a Business Associate, and may allow a Business Associate to create or receive patient health information on VUOM's behalf, only if the Business Associate agrees in writing to, among other things, safeguard such information. As such, VUOM personnel are prohibited from disclosing to a Business Associate, or permitting a Business Associate to create or receive on behalf of VUOM, any patient health information until VUOM and the Business Associate enter into an appropriate written agreement.

**BUSINESS ASSOCIATES**

**Procedures**

**A. Identifying Business Associates:** In order to assist VUOM personnel in identifying Business Associates, the following guidelines apply:

1. Business Associates do not include members of VUOM's workforce (i.e. an employee, volunteer, trainee, or other person whose conduct, in the performance of work for VUOM, is under VUOM's direct control, whether or not they are paid by VUOM).
2. Business Associates include individuals or entities who, on behalf of VUOM (other than in the capacity of a member of VUOM's workforce), perform, or assist in the performance of a function or activity involving the use or disclosure of patient health information (e.g., claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing) or any function or activity regulated by HIPAA.
3. Business Associates include individuals or entities who provide (other than in the capacity of a member of VUOM's workforce) legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for VUOM where the provision of the service involves the disclosure of patient health information from VUOM, or from another Business Associate of VUOM.
4. Questions regarding whether an individual or entity is a Business Associate should be directed to the Privacy Officer.

**Examples of potential Business Associates:**

Service Providers

- Accountants
- Attorneys
- Coding providers
- Collection service companies
- Transcription service companies
- Microfilm conversion providers
- Clearinghouse
- Billing companies
- Data backup/storage companies
- Document storage companies
- Practice management companies
- Temporary staffing agencies
- Medical Directors
- Physician teaching arrangements
- Teaching affiliation arrangements



Examples of individuals and entities who are not Business Associates:

- Members of VUOM's workforce
- An entity that performs services as part of an Organized Health Care Arrangement in which VUOM participates
- Construction, maintenance and repair services
- Courier services (i.e., U.S. Post Office, FedEx, UPS, etc.)
- Financial institutions that merely process patients' payments for health care

## B. Procedures

1. **Identifying Business Associates:** The Privacy Officer and VUOM's Privacy Committee are responsible for assisting in identifying those vendor contracts that require HIPAA Business Associate provisions and ensuring that such contracts are amended appropriately. Unless otherwise approved by the Privacy Officer, VUOM's Model Business Associate Addendum, a copy of which is included in Appendix C of this Manual, should be executed contemporaneous with all new Business Associate contracts.
2. **Contract Review:** The Privacy Officer or his/her designee must review any proposed new contract with an existing or potential Business Associate to ensure that required Business Associate provisions are included in the contract. The Privacy Officer should also consider whether the contract with the Business Associate should contain any additional language required by the other HIPAA regulations (e.g., security, transaction and code sets).
3. **Prohibited Activities:** VUOM personnel are prohibited from disclosing patient health information to a Business Associate, or permitting a Business Associate to create or receive patient health information on VUOM's behalf, unless the representatives of both VUOM and the Business Associate sign a contract that contains the required Business Associate provisions.
4. **Contract Maintenance:** Upon execution, a copy of the Business Associate contract must be sent to the Privacy Officer. The Privacy Officer is responsible for maintaining a copy of all such contracts in a centralized location.
5. **Reporting a Suspected Breach by a Business Associate:** If any VUOM personnel believes that a Business Associate has breached any of its obligations with respect to patient health information, such personnel must report his or her belief to the Privacy Officer as soon as possible.
6. **Curing Breach by Business Associate:** If, after investigation, the Privacy Officer believes that the Business Associate breached its obligations with respect to patient health information (e.g., inappropriately used or disclosed such information, failed to provide access to patient health information, etc.), the Privacy Officer or the Privacy Officer's designee should attempt to have the Business Associate cure the breach and if such steps are unsuccessful:
  - a. Terminate the contract or arrangement, if feasible; or
  - b. If termination is not feasible, report the problem to the Secretary of the U.S. Department of Health and Human Services.

## HANDBOOK ACKNOWLEDGEMENT

The University provides all faculty members and student interns with a hard copy of the University's Clinic HIPAA Privacy Handbook. This handbook works as a guide to policies, procedures, benefits, and general information. I understand that I should consult the Clinic Director regarding any questions not answered or covered in this handbook.



Since the information and policies described here are necessarily subject to change, I acknowledge that revisions to the handbook may occur. All such changes will be communicated through official notices, and I understand that revised information may supersede, modify, or eliminate existing policies. Only the Clinic Director, with the final approval of the President of the College has the ability to adopt any revisions to the policies in this handbook.

I acknowledge that my responsibility to the Institution is to comply with the policies contained in this handbook and any revisions made to it. Any information within is the property of the College.

---

**Faculty or Student Intern Name (printed):**

---

**Faculty or Student Intern Signature:** **Date:**



**APPENDIX**

- 1. Notice of HIPAA Privacy Practices**
- 2. Acknowledgement of Notice of HIPAA Privacy Practices**
- 3. Consent Form**



**NOTICE OF HIPAA PRIVACY PRACTICES**  
Virginia University of Oriental Medicine (VUOM)  
Acupuncture Clinic  
9401 Mathy Dr. • Fairfax, VA 22031

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU MAY ACCESS THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.**

This Notice is provided to you pursuant to the Health Insurance Portability and Accessibility Act of 1996 and its implementing regulations (HIPAA). It is designed to tell you how we may, under federal law, use or disclose your Health Information.

**I. We May Use or Disclose Your Health Information for Purposes of Treatment, Payment or Healthcare Operations without Obtaining Your Prior Authorization and Here is One Example of Each:**

1. We may provide your Health Information to health care professionals including doctors, nurses and technicians -- for purposes of providing you with care.
2. Our billing department may access your information and send relevant parts to other insurance companies to allow us to be paid for the services we render to you.
3. We may access or send your information to our attorneys or accountants in the event we need the information in order to address one of our own business functions.

**II. We May Also Use or Disclose Your Health Information Under the Following Circumstances without Obtaining Your Prior Authorization:**

1. To Notify and/or Communicate with your Family. Unless you tell us you object, we may use or disclose your Health Information in order to notify your family or assist in notifying your family, your personal representative or another person responsible for your care about your location, your general condition or in the event of your death. If you are unable or unavailable to agree or object, our health professionals will use their best judgment in any communications with your family and others.
2. As Required by Law.
  - For Public Health Purposes: We may use or disclose your Health Information to provide information to state or federal public health authorities, as required by law to prevent or control disease, injury or disability; to report child abuse or neglect; report domestic violence; report to the Food and Drug Administration problems with products and reactions to medications; and report disease or infection exposure.
  - For Health Oversight Activities: We may use or disclose your Health Information to health agencies during the course of audits, investigations, certification and other proceedings.
  - In Response to Subpoenas or for Judicial and Administrative Proceedings. We may use or disclose your Health Information in the course of any administrative or judicial proceeding. However, in general, we will attempt to ensure that you have been made aware of the use or disclosure of your Health Information prior to providing it to another person.
  - To Law Enforcement Personnel. We may use or disclose your Health Information to a law enforcement official to identify or locate a suspect, fugitive, material witness or missing person, comply with a court order or subpoena and other law enforcement purposes.
  - To Coroners or Funeral Directors. We may use or disclose your Health Information for purposes of communicating with coroners, medical examiners and funeral directors.
  - For Purposes of Organ Donation. We may use or disclose your Health Information for purposes of communicating to organizations involved in procuring, banking or transplanting organs and tissues.
  - For Public Safety. We may use or disclose your Health Information in order to prevent or



lessen a serious and imminent threat to the health or safety of a particular person or the general public.

- To Aid Specialized Government Functions. If necessary, we may use or disclose your Health Information for military or national security purposes.
- For Worker's Compensation. We may use or disclose your Health Information as necessary to comply with worker's compensation laws.
- To Correctional Institutions or Law Enforcement Officials, if You are an Inmate.

**III. For All Other Circumstances, We May Only Use or Disclose Your Health Information After You Have Signed an Authorization. If you authorize us to use or disclose your Health Information for another purpose, you may revoke your authorization in writing at any time.**

**IV. You Should Be Advised that We May Also Use or Disclose Your Health Information for the Following Purposes:**

1. Appointment Reminders. We may use your Health Information in order to contact you to provide appointment reminders or to give information about other treatments or health-related benefits and services that may be of interest to you.
2. Change of Ownership. In the event that our entity is sold or merged with another organization, your Health Information/record will become the property of the new owner.
3. Providing Information to Our Plan Sponsor [If a Health Plan]. We may disclose your Health Information to our Plan Sponsor.

**V. Your Rights**

1. You have the right to request restrictions on the uses and disclosures of your Health Information. However, we are not required to comply with your request.
2. You have the right to receive your Health Information through confidential means through a reasonable alternative means or at an alternative location.
3. You have the right to inspect and copy your Health Information. We may charge you a reasonable cost-based fee to cover copying, postage and/or preparation of a summary.
4. You have a right to request that we amend your Health Information that is incorrect or incomplete. We are not required to change your Health Information and will provide you with information about our denial and how you can disagree with the denial.
5. You have a right to receive an accounting of disclosures of your Health Information made by us, except that we do not have to account for disclosures: authorized by you; made for treatment, payment, health care operations; provided to you; provided in response to an Authorization; made in order to notify and communicate with family; and/or for certain government functions, to name a few.
6. You have a right to a paper copy of this Notice of Privacy Practices. If you would like to have a more detailed explanation of these rights or if you would like to exercise one or more of these rights, contact:

Hyung Sik Byeon, L.Ac., VUOM Director of Clinical Operations  
Virginia University of Oriental Medicine (VUOM) • Acupuncture Clinic  
9401 Mathy Dr. Suite101 • Fairfax, VA 22031  
Phone No. (703) 323-5691 • Fax No. (703) 323-5692 • Website: [www.vuom.org](http://www.vuom.org)



**VI. Our Duties.**

1. We are required by law to maintain the privacy of your Health Information [and to provide you with a copy of this Notice.]
2. We are also required to abide by the terms of this Notice.
3. We reserve the right to amend this Notice at any time in the future and to make the new Notice provisions applicable to all your Health Information  $\Delta$  even if it was created prior to the change in the Notice. If such amendment is made, we will immediately display the revised Notice at our office and provide you with a copy of the amended Notice. We will also provide you with a copy, at any time, upon request.

**VII. Complaints to the Government.**

You may make complaints to the Secretary of the Department of Health and Human Services (DHHS) if you believe your rights have been violated.

We promise not to retaliate against you for any complaint you make to the government about our privacy practices.

**VIII. Contact Information.**

You may contact us about our privacy practices by calling the Privacy Officer,

Hyung Sik Byeon, L.Ac., VUOM Director of Clinical Operations  
 Virginia University of Oriental Medicine (VUOM) • Acupuncture Clinic  
 9401 Mathy Dr. Suite 101 • Fairfax, VA 22031  
 Phone No. (703) 323-5691 • Fax No. (703) 323-5692 • Website: [www.vuom.org](http://www.vuom.org)

You may contact the DHHS at:

U.S. Department of Health & Human Services, 200 Independence Avenue, S.W. , Washington, D.C. 20201,  
 Telephone: 202-619-0257, Toll Free: 1-877-696-6775

I have received a copy of this Health Insurance Portability and Accessibility Act (HIPAA) NOTICE OF PRIVACY PRACTICES. I have been informed whom to contact if I need more information.

Patient Name (print) \_\_\_\_\_

Patient Signature \_\_\_\_\_ Date \_\_\_\_\_



**ACKNOWLEDGEMENT OF RECEIPT OF:  
NOTICE OF HIPPA PRIVACY PRACTICES**

1. As required by the HIPPA Privacy Regulations, I hereby acknowledge that I have received a copy of VUOM's *Notice of HIPPA Privacy Practices*.
2. As required by HIPPA Privacy Regulations,

Mr / Ms. \_\_\_\_\_,

from Virginia University of Oriental Medicine Acupuncture Clinic, has explained the *Notice of HIPPA Privacy Practices* to my satisfaction. As required by the HIPPA Regulations, I am aware that Virginia University of Oriental Medicine Acupuncture Clinic has included a provision that it reserves the right to change the terms of its notice and to make those changes effective for all protected health information that it maintains.

Patient  
Name (print) \_\_\_\_\_

Patient  
Signature \_\_\_\_\_ Date \_\_\_\_\_



**\*\*\*OFFICE USE ONLY\*\*\***

Signed form  
received by: \_\_\_\_\_

Good faith effort to  
Obtain receipt: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



CONSENT FORM

“Acupuncture” means the stimulation of a certain point or points near the surface of the body by the insertion of special needles. The purpose of acupuncture is to prevent or modify the perception of pain and is thus a form of pain control. In addition, through the normalization of physiological functions, it may also serve in the treatment of certain diseases or dysfunctions of the body. Acupuncture includes the techniques of electro-acupuncture (the therapeutic use of weak electric currents at acupuncture points), mechanical stimulation (stimulation of an acupuncture point or points on or near the surface of the body by means of apparatus or instrument), and moxibustion (the therapeutic use of thermal stimulus at acupuncture points by burning Artemisia alone or Artemisia formulations).

The potential risks: slight pain or discomfort at the site of needle insertion, infection, bruises, weakness, fainting, nausea, and aggravation of problematic systems existing prior to acupuncture treatment.

The potential benefits: acupuncture may allow for the painless relief of one’s symptoms without the need for drugs, and improve balance of bodily energies leading to the prevention of illness, or the elimination of the presenting problem.

Please Note: The acupuncture treatment (which includes procedures described above) that you will receive today and in the future, at the Intern Clinic of Virginia University of Oriental Medicine, will be carried out by a student(s) in his/her third year of acupuncture training. This means that the student(s) treating you is NOT a licensed acupuncturist, and is not yet qualified to perform acupuncture treatments outside the Intern Clinic. However, the student(s) is closely supervised by an acupuncturist who is licensed to practice acupuncture in the state of Virginia.

**I hereby consent to be treated with Acupuncture administered by Virginia University of Oriental Medicine student intern under supervision of a Clinic Supervisor L.Ac. I understand and accept that no guarantee is made concerning the outcome of my Acupuncture treatments, and I understand that I may stop treatment at any time.**

\_\_\_\_\_  
Patient signature

\_\_\_\_\_  
Date