American College of Traditional Chinese Medicine Clinic

Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Privacy Manual

ACTCM

American College of Traditional Chinese Medicine
at California Institute of Integral Studies

August 2017

TABLE OF CONTENTS

HIPAA AND PRIVACY POLICIES

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law which, in part, protects the privacy of individually identifiable patient information, provides for the electronic and physical security of health and patient medical information, and simplifies billing and other electronic transactions and code sets. HIPAA privacy and security standards were updated in 2009 by the Health Information Technology for Economic and Clinic Health (HITECH) Act and in 2013 by the HIPAA Final Omnibus Rule.

Protected Health Information (PHI) is information that is created or received by ACTCM Clinic and relates to the past, present, or future health condition of a patient; the provision of health care to patient; or the past, present or future payment for the provision of health care to a patient; and that identifies the patient or for which there is reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased.

Examples of PHI are:

- Patient's chart number
- Patient's demographic information (e.g. address, phone number, email address)
- Patient's image
- Information written in a patient's medical chart that can be linked to the patient
- Information about a patient in a provider's computer system
- Patient's billing information
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

The Standards set forth by HIPAA apply to "covered entities," including health care providers and the agencies they work within. The ACTCM Clinic is a covered entity and is thus required to comply with the regulation specified by HIPAA. This manual details the policies and procedures established for the ACTCM Clinic to ensure HIPAA compliance.

I. GENERAL RESPONSIBILITIES AS A COVERED ENTITY

A. ACTCM CLINIC PRIVACY OFFICER

The Clinic Operations Director is the designated Privacy Officer and is responsible for knowing HIPAA regulations, training the Clinic staff, in HIPAA compliance, and assuring that HIPAA-related policies and procedures are instituted and followed. The Clinic Operations Director will:

- Update HIPAA policies and procedures
- Oversee the implementation of the policies and procedures contained in this Manual
- Developing and maintaining a Notice of Privacy Policies (NPP) for patients
- Ensure that all Clinic staff are trained regarding HIPAA and the policies and procedures of the Clinic
- Provide HIPAA education materials to clinic and didactic faculty to train student clinicians
- Review activity that takes place in the Clinic to detect security risks
- Serve as the contact person for patients who have questions, concerns, or complaints about the privacy of their PHI
- Investigate and respond to privacy related incidents and take appropriate action in the event of a breech in privacy, and eliminate or mitigate any damaging effects

B. PRIVACY INCIDENT RESPONSE TEAM

The Privacy Incident Response Team (PIRT) is compromised of the Privacy Officer (Clinic Operations Director), Director of Clinical Education, Assistant Director of Clinical Education, Assistant Clinic Operations Director and additional members deemed appropriate pursuant to the incident. Because customer service and privacy are of utmost importance to ACTCM, it is our policy to promptly receive, respond, and resolve patient complaints regarding allegations of improper use or disclosure of PHI by ACTCM or our business associates.

1. Formal Patient Complaints: An individual may submit a written formal complaint about ACTCM Clinic's privacy practices, including but not limited to complaints regarding:
    - The privacy and security of PHI;
    - Use and disclosure of PHI;
    - Patients' access to, or amendment of, their PHI;
    - Practices or actions of ACTCM's business associates;
    - ACTCM's marketing practices; or
    - Any other complaint relating to ACTCM's privacy policies and procedures.

2. Processing Patient Complaints: The Privacy Officer receives the complaint and fills out the ACTCM Incident Form attaching the written formal complaint and forwards it to the members of PIRT to take appropriate actions to prevent further inappropriate incidents.

ACTCM must maintain complete documentation of the complaint and PIRT's review and disposition of the matter, including a record of any changes to policies or procedures or the imposition of actions involving staff, faculty or students, if any. ACTCM must retain all documents relating to the complaint and the investigation for a period of at least seven years from the date of the incident.

3. Internal Privacy Violation Reviews: ACTCM staff, faculty and students are encouraged to report violations of federal and state privacy laws and ACTCM's privacy policies ("Privacy Violations") to ACTCM's Privacy Officer. Whenever possible privacy violations arise, the Privacy Officer along with PIRT will conduct an investigation and determine whether a violation has occurred. If PIRT determines that a staff or faculty member student of business associate has committed a Privacy Violation, that person shall be subject to appropriate actions as determined by PIRT, Clinic Dean, Director of Human Resources, or any appropriate manager or supervisor. Even if no actual privacy violation has occurred, disciplinary measures may be imposed if otherwise warranted by the circumstances. The actions imposed may include, but are not limited to, informal counseling, verbal warning, written warning, or other sanctions deemed appropriate by Privacy Officer in consultation with the Director of Clinical Education. In all cases, the actions imposed will be in the discretion of these managers. However, in most cases the consequences will depend on the seriousness of the offense. A record of the event and any discipline imposed shall be maintained in the staff or faculty personnel file or the student academic file with a copy to be filed in a master file maintained by the Privacy Officer. In all cases where there are administrative penalties pending by the United States Department of Health and Human Services or some other entity outside of ACTCM, including possible legal action, the Director of Clinical Education must inform the Academic Council.

4. Types of Possible Actions for Privacy Violations: The type of discipline actions imposed will generally reflect the seriousness of the violation. Factors may include the severity, frequency, degree of deviation from expectations, and length of time involved in any privacy violations.

a. Informal Counseling: PIRT or an appropriate supervisor may engage in an informal counseling with respect to privacy issues that does not warrant more severe sanctions. Documentation of informal counseling will be maintained in the Clinic's Incident File.

b. Verbal Warning: PIRT or an appropriate supervisor may issue a verbal warning. Documentation of the verbal warning in the form of meeting notes will be maintained in the Clinic's Incident File.

c. Written Warning: PIRT or an appropriate supervisor may issue a written warning. Such a warning may be appropriate, for example, when the behavior is a repeated violation and verbal counseling has been administered, or the violation is more serious in

nature and/or subjects ACTCM to legal liability. Written warnings will be documented in personnel, departmental or academic files.

d. Other Sanctions: In appropriate circumstances, other sanctions can be issued that are deemed appropriate. A written description of the behavior that resulted in the sanction and the required behavioral or performance objectives that must be met in future will be kept in personnel, departmental or academic files.

C. HIPAA COMPLIANCE TRAINING

It is ACTCM's policy to provide training to all staff, faculty, and students who have access to PHI on its privacy policies and procedures and to ensure that education curriculum and materials are created and maintained to provide adequate training to students to properly handle PHI during their clinical hours. Privacy training will review ACTCM's privacy policies and procedures and will discuss any changes in these policies and procedures. The training program will focus on federal laws and regulations governing the privacy, confidentiality, and security of PHI, as well as any important and relevant state laws.

1. ACTCM Clinic Staff Training: ACTCM Clinic managers and staff attended HIPAA training in conjunction with a year-end staff meeting. As a part of their orientation, new staff members that have access to PHI are asked to sign ACTCM's Privacy and Confidentiality Agreement Form. If a current or new staff member has any questions or concerns with ACTCM's HIPAA compliance or privacy policies, they may meet with the Privacy Officer. Privacy training is mandatory for all ACTCM Clinic staff and will meet with the Privacy Officer to discuss privacy policies and procedures and read the HIPAA Manual before performing any clinical duties. ACTCM Clinic staff sign the Confidentiality Agreement Form twice a year, and the signed Confidentiality Agreement Forms are placed in a secure binder located at the Privacy Officer's Desk.

2. ACTCM Faculty Training: ACTCM Clinic faculty attended HIPAA training biannually in conjunction with a quarterly faculty meeting. As a part of their orientation, new faculty are given an ACTCM HIPAA Fact Sheet and asked to sign ACTCM's Privacy and Confidentiality Agreement Form. If a current or new faculty member has any questions or concerns with ACTCM's HIPAA compliance or privacy policies, they may meet with the Privacy Officer. ACTCM Clinic faculty sign the Confidentiality Agreement Form twice a year, and the signed Confidentiality Agreement Forms are placed in a secure binder located at the Privacy Officer's Desk.

3. ACTCM Student Training: Education curriculum and materials are created and maintained to provide adequate training to students to properly handle PHI during their clinical hours:

a. In ACM 5112 Clinical and Program Orientation course, HIPAA and ACTCM's privacy policies are reviewed and discussed and the Privacy Officer meets with the class to answer any questions or concerns.

b. In ACM 5250 Clinic Observer I/Clinic Theater course, HIPAA and ACTCM's privacy policies are reviewed, students sign ACTCM's Privacy and Confidentiality Agreement Form. The signed Confidentiality Agreement Forms are placed in a secure binder located at the Privacy Officer's Desk.

c. Clinic faculty and staff review the current privacy policies with student clinicians at the beginning of each semester. Clinic students sign ACTCM's Privacy and Confidentiality Agreement Form twice a year. The signed Confidentiality Agreement Forms are placed in a secure binder located at the Privacy Officer's Desk.

d. The Privacy Officer is available to meet with students throughout their clinical training to answer any questions or concerns with HIPAA or ACTCM's Privacy Policies.

4. Additional Training: When changes are made to a policy or procedure, all staff, faculty and students whose functions are affected by the change must receive training on the new policies and procedures within 60 days after the change has been made. Additional training sessions may be conducted for specific individuals who have responsibilities involving specific compliance issues. In addition, the Privacy Officer may direct specific employees to attend privacy training if he or she believes that such training is warranted.

5. Training Documentation: The Privacy Officer will document any training that has been provided.

6. Access to PHI is limited to certain staff, faculty and students: All staff, faculty and students will have access to PHI as determined by their department, job description or clinical training level. Unauthorized staff, faculty, and students may not access PHI either through the MediSoft electronic program, patient ledger cards or patient medical charts that includes medical and/or demographic information for family members, friends, other staff, faculty or students or other individuals for personal or other non-work related or clinical educational purposes.

II. NOTICE OF PRIVACY PRACTICE

ACTCM provides each new patient with a Notice of Privacy Practice ("NPP") and requires them to read and sign an acknowledgement of receipt of notice of privacy practices on their first visit. In addition, the NPP is posted in plain in plain view of the Clinic waiting room and will make the NPP available to all patients upon request.

A. PATIENT'S RIGHT TO A NOTICE OF PRIVACY PRACTICE

The NPP must be written in plain language, and if a use or disclosure is prohibited by state law, the NPP's description of such use or disclosure must reflect the state law. Patients have the right to adequate notice of:

1. The uses and disclosures of PHI that may be made by ACTCM;

2. The patient's rights with respect to PHI; and

3. ACTCM's legal obligations regarding PHI.

The NPP will also provide a description of ACTCM's complaint procedures in regards to privacy issues, the name and phone number of the Privacy Officer, and the date of the notice.

B. ACTCM'S PROVISION OF THE NOTICE TO PATIENTS

ACTCM will provide a paper copy of the NPP to patients and the public in general.

1. ACTCM must make the NPP available upon request to any person, even if they are not a current patient.

2. ACTCM must provide the NPP to the patient no later than the date that ACTCM first provides service to the patient. The ACTCM may send the NPP to all of its patients at once, give the notice to each patient as he or she comes into the Clinic or by any combination of these approaches.

3. ACTCM must have the NPP available at the clinic for individuals to request to take with them.

4. ACTCM must post the NPP in a prominent location in the clinic where patients will be able to read it.

C. REVISION TO THE NOTICE

ACTCM must promptly revise and distribute its NPP whenever there is a change to the uses or disclosures of PHI, the individuals' rights, ACTCM's legal obligations, or other privacy practices stated in the NPP.

1. Whenever the NPP is revised, ACTCM must make the NPP available upon request on or after the effective date of the revision, promptly make the NPP available at the clinic, and post the revised NPP in a prominent location in the clinic.

2. After giving a patient a copy of the NPP upon his or her first visit ACTCM is not required to further distribute the NPP to the patient unless requested. Even if ACTCM revises the NPP, it is not required to distribute the NPP to all current and former patients. ACTCM only has to make the NPP available upon request and post the information in the clinic.

D. NOTICE OF PRIVACY PRACTICES RETENTION REQUIREMENT

ACTCM must retain a copy of each NPP it issues for a period of seven (7) years from the date that the NPP was last in effect.

III. AUTHORIZATION FOR USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)

ACTCM will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclose" are defined as follows:

- Use- The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any ACTCM staff, faculty or student or ACTCM Business Associate; and
- Disclose- For information that is PHI, disclosure means any release, transfer, provision or access to, or divulging in any other manner of individually identifiable health information to persons not an ACTCM staff, faculty or student with a business or educational need to know PHI.

ACTCM must obtain a valid, signed authorization form from a patient prior to using or disclosing the patient's PHI for any purpose that satisfies all HIPAA's requirement or the rules that allow uses or disclosures without the patient's permission.

A. WHEN AUTHORIZATION IS REQUESTED

Prior authorization is required before ACTCM uses or discloses PHI for "non-routine" purposes beyond treatment or health care operations, such as sales of PHI and certain marketing activities. Among the uses and disclosures for which an authorization is not required are the following:

- For treatment, payment, and health care operations;
- For public health activities;
- About victims of abuse, neglect, or domestic violence;
- For health oversight activities;
- For judicial and administrative proceedings;
- For law enforcement purposes;
- About decedents;
- For certain research purposes where a waiver has been obtained;
- To avert a serious threat to health or safety;
- For specialized government functions;
- For workers' compensation;
- To the Department of Health and Human Services for enforcement of the privacy rules; and
- For certain marketing communications.

B. AUTHORIZATION CONTENT REQUIREMENTS

All authorizations must be written in "plain language." This means that ACTCM must make a reasonable effort to:

- Organize material to serve the needs of the reader
- Write short sentences in the active voice, using "you" and other pronouns
- Use common, everyday words in sentences

- Divide material into short sections

1. All authorizations 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 name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure.

   c. The name or other specific identification of the person(s) or class of persons to whom ACTCM will disclose the information.

   d. A description of each purpose of the requested use or disclosure with enough information to allow patients to make informed decisions about whether to release the information. Broad or blanket authorizations requesting the use or disclosure of PHI for a wide range of unspecified purposes are prohibited, but if the patient is initiating the authorization the purpose may be described as "at the request of the individual."

   e. An expiration date or an expiration event that relates to the patient or the purpose of the use or disclosure. The authorization may expire on a specific date, a specific time period (e.g., 3 years from the date of the signature), or an event directly relevant to the patient or the purpose of the use or disclosure (e.g., for the duration of the patient's treatment for a specific condition). Authorizations may not have an unspecified expiration date.

   f. Patient signature and date.

   g. If the authorization is signed by a personal representative of the patient, a description of the representative's authority to act for the patient.

2. In addition to the core, authorizations must contain all of the following notifications:

   a. A statement that the patient has the right to revoke the authorization in writing and either a discussion of the exceptions to the right to revoke, together with a description of how the patient may revoke the authorization, or, to the extent that this information is included in the NPP.

   b. For most authorizations, a statement that ACTCM will not condition treatment, payment, or eligibility on the patient's providing authorization for the requested uses or disclosures.

   c. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the Privacy Regulations.

C. AUTHORIZATION FOR MARKETING

If the authorization is for marketing purpose, and the marketing involves any direct or indirect compensation to ACTCM from a third party, the authorization must state this fact. ACTCM uses limited amount of PHI for marketing purposes.

D. COPY TO THE PATIENT

The ACTCM must give the patient a copy of the signed authorization.

E. INVALID AUTHORIZATIONS

An authorization is not valid if it has any of the following defects:

1. The expiration date has passed or the expiration event is known by ACTCM to have occurred.

2. The required elements of the authorization have not been filled out completely.

3. The authorization is known by ACTCM to have been revoked.

4. The authorization lacks a required element.

5. Any material information in the authorization is known by ACTCM to be false.

F. CANCELATION OF AUTHORIZATIONS

A patient may revoke an authorization at any time by means of a written revocation, except to the extent that ACTCM has taken action in reliance upon the authorization. When a patient revokes an authorization, ACTCM must stop making uses and disclosures pursuant to the authorization to the greatest extent practical.

G. RECORD RETENTION REQUIREMENTS

ACTCM must document and retain signed authorizations for seven years after the date they were last in effect.

IV. GENERAL USE AND DISCLOSURE POLICY

ACTCM will use and disclose PHI only as specifically permitted or required by the privacy rules in accordance with the ACTCM's privacy policies and procedures.

A. INTRODUCTION

Basic rules for use and disclosure of PHI: Faculty, staff or students may not use or disclose PHI unless permitted or required by these privacy rules.

1. Permitted uses and disclosures of PHI are:

a. To the patient;
b. To carry out treatment, payment or health care operations;
c. In compliance with a valid authorization;
d. Pursuant to a verbal agreement from a patient that permits disclosure to a caregiver; and
e. For disclosures required by law and permitted under HIPPA.

2. Incidental uses and disclosures that occur as a by-product of a use or disclosure otherwise permitted under the privacy rules are explicitly permitted, so long as ACTCM has applied reasonable safeguards and implemented the minimum necessary standard, where applicable.

B. MINIMUM NECESSARY

1. The Minimum Necessary Standard: When using or disclosing PHI, and when requesting PHI from another entity, ACTCM must make reasonable efforts to use, disclose or request the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure or request.

2. Exceptions: Among the uses, disclosures, and requests to which the minimum necessary standard does not apply are:
   a. Uses and disclosures for treatment purposes;
   b. Disclosures to the patient who is the subject of the information;
   c. Most uses or disclosures made pursuant to an authorization;
   d. Uses or disclosures made in mandatory or situational occurrences of a HIPAA transactions standard;
   e. Disclosures to HHS when required by HHS for compliance and enforcement purposes; and
   f. Uses or disclosures that are required by other law.

3. Required Policies and Procedures for Uses of PHI: ACTCM must develop and implement policies that limit the use of PHI to the minimum PHI reasonably necessary to accomplish the intended purpose of the use or disclosure. The policies and procedures for use of PHI must identify:
   a. The persons or classes of persons in the College who need access to PHI to carry out their duties;
   b. The categories of PHI that each person or class of person's needs; and
   c. Any conditions necessary for such access.

   ACTCM must have policies and procedures that limit access to only the identified persons and to only the identified PHI. These policies and procedures should be based on reasonable determinations about the persons or classes of persons who require PHI, and the nature of the PHI they require, for their particular job responsibilities.

4. Required Policies and Procedures for Disclosures of PHI: ACTCM also is required to develop certain policies and procedures for disclosures of PHI. The regulatory

requirements differ depending on whether the disclosure is a routine or non-routine disclosure.

a. For any type of disclosure that is made on a routine, recurring basis, ACTCM must develop and implement policies and procedures (which may be standard protocols) that permit only the disclosure of the minimum amount of PHI that is reasonably necessary to achieve the purpose of the disclosure. These policies are drafted by the Privacy Officer and approved by the Dean of Clinical Education. Should such policy be developed in response to an incident or complaint, the President's Council will be informed by the Dean. The policies and procedures must identify the:
    i. Types of PHI to be disclosed;
    ii. Types of persons who may receive the PHI; and
    iii. Conditions necessary for such access.
b. For non-routine disclosures, ACTCM must develop reasonable criteria for determining and limiting disclosure to only the minimum amount of PHI necessary to accomplish the purpose of the disclosure.

    The factors that may be considered in making such a determination are:
    i. How much PHI will be disclosed?
    ii. To what extent would the disclosure increase the number of persons with access to the PHI?
    iii. What is the likelihood of further disclosures?
    iv. How important is the disclosure?
    v. Can substantially the same purpose be achieved using de-identified information?
    vi. Is there technology available to limit the amount of PHI disclosed?
    vii. What is the cost, financial or otherwise, of limiting the disclosure?
    viii. Who is making the request?

ACTCM must also develop and implement procedures for reviewing non-routine requests for disclosures on an individual basis in accordance with established criteria.

5. Requests for PHI: The minimum necessary standard applies to situations where the ACTCM is requesting an individual's PHI from another entity.

a. For requests to other entities made on a routine and recurring basis, ACTCM must establish standard protocols describing what information is reasonably necessary for the purposes for which it is requested, and limit its requests to only that information.
b. For non-routine requests, ACTCM must develop policies and procedures that provide for review of the requests on an individualized basis.

6. Reasonable reliance on requested disclosures: ACTCM may rely, if reasonable under the circumstances, on statements by public officials or other covered entities or their business associates that they are requesting the minimum PHI necessary to achieve the stated purpose of the request. ACTCM may also reasonably rely on the statements of its own business associates or professionals within its workforce (such as attorneys or accountants) that the information requested to provide professional services ACTCM is the minimum necessary for such purposes.

C. DE-IDENTIFICATION

1. Basic standard: Health information is considered de-identified (i.e. not individually identifiable) under the rules if it does not identify a patient and ACTCM has no reasonable basis to believe it can be used to identify a patient. De-identified information is not PHI and therefore the requirements of the rules do not apply to such information.

1. De-identifying information: ACTCM may de-identify information in two ways:
   a. If a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering information not individually identifiable makes a determination, and documents the analysis, that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information; or

   b. If ACTCM removes a list of specified identifying information about the individual or his or her relatives, employers, or household members, and ACTCM has no actual knowledge that the information could be used alone or in combination to identify a subject of the information.

2. Use of PHI to create de-identified information: ACTCM may use PHI to create de-identified information, or may disclose PHI to a business associate for such purpose, whether or not the de-identified information will be used ACTCM.

3. No PHI may be photocopied by faculty without prior written permission of the Privacy Officer or the Director of Clinical Education. All such photocopies must be redacted.

4. No student may photocopy PHI at any time.

D. DISCLOSURE TO FRIENDS AND FAMILY

ACTCM may disclose to a person involved in the current health care of the patient (such as a relative, close personal friend, or any other person identified by the patient) PHI directly related to the person's involvement in the current health care of the patient or payment for the patient's health care. Examples of persons who might be involved in the patient's care include, but are not limited to:

- Blood relatives;
- Spouses;
- Roommates;
- Domestic partners; and
- Neighbors.

1. Disclosures of PHI when the patient is present: When the patient is present and has the capacity to make his or her own decisions, ACTCM may disclose PHI to the third party only if ACTCM:

a. Obtains the patient's agreement to disclose to the third party involved in his or her care;

b. Provides the patient with an opportunity to object to such disclosure and the patient does not express an objection; or

c. Reasonably infers from the circumstances, based on the exercise of professional judgment that the patient does not object to the disclosure.

2. Disclosures of PHI when the patient is not present: When a patient is not present (e.g. when a spouse of the patient seeks to pick up the patient's herbs at ACTCM) or when ACTCM cannot practically give the patient an opportunity to agree or object to the use or disclosure (e.g., because of the patient's incapacity or an emergency circumstance), ACTCM may, in the exercise of professional judgment, determine whether the disclosure is in the patient's best interests and if so, disclose only the PHI that is directly relevant to the person's involvement with the patient's health care. For instance, this allows the clinic to disclose instructions for taking a particular herbal formula to an elderly patient's family member. Where possible the patient will be asked to request in writing which family members or care givers may receive PHI from ACTCM. The clinic must follow these guidelines when deciding whether to disclose PHI when the patient is not present:

a. Only disclose PHI that is directly related to the patient's current condition.

b. Consider the patient's best interests and construe this opportunity narrowly, allowing disclosures only to those persons with close relationships with the patient, such as family members.

c. Take into account whether the disclosure is likely to put the patient at risk of serious harm.

d. ACTCM staff, faculty and students are not required to verify the identity of relatives or other persons involved in the patient's care.

e. A patient's agreement to disclosure of PHI in one situation or on one occasion does not mean that the patient is agreeing to disclosures of PHI indefinitely in the future. Use professional judgment to determine the scope of the person's involvement in the patient's care and the time period during which the patient agrees to the other person's involvement.

E. VERBAL COMMUNICATIONS

The rules apply to PHI in all forms such as electronic, written, verbal, and any other form.

1. Use of PHI in verbal communications: ACTCM staff, faculty and students may discuss a patient's PHI over the telephone with the patient, or designated representative. Should

staff, faculty or a student call a patient's number and get a voicemail greeting they may only leave a message with limited general information.

2. Documentation of verbal communications: ACTCM is not required to document any information, including verbal information, which is used or disclosed for treatment, payment, or health care operations. However, where the rules or ACTCM's privacy policies require documentation of other types of disclosures, verbal communications are included in this requirement. For example, verbal disclosures of PHI for purposes other than treatment, payment, or health care operations must be documented in order to provide the patient with a complete accounting of disclosures.

3. Staff, faculty and students' duty to safeguard PHI: Staff, faculty and students must reasonably safeguard PHI, including verbal information, from any intentional or unintentional use or disclosures that are in violation of the rules or ACTCM's privacy policies. This means that authorized personnel must make reasonable efforts to prevent improper uses and disclosures of PHI. Measures that ACTCM takes to protect patients' privacy include:

    a. Refrain from discussing cases in the hallways, waiting area, patio area or front desk.

    b. Making available treatment rooms where the clinicians can counsel patients regarding treatment of their medical conditions including use of herbs.

    c. Speaking quietly or asking that waiting patients stand a few feet back from the counter when ACTCM staff, faculty and students are consulting with patients from behind the front desk counter.

    d. Telephone calls made in the reception area should generally be for routine appointment reminders and appointment clarification, and only first names should be used.

    e. Keep the volume at an appropriate level over the phone so conversations cannot be overheard. Telephone calls requiring sensitive information or more disclosure should be made from the Faculty Office or Herbal Dispensary.

    f. Avoid leaving any PHI or other sensitive information on voicemail messages.

    g. When treating patients in a community setting such as at Ear Clinics and outreach events, speak quietly and keep volume at an appropriate level so conversations cannot be easily overheard. Keep discussion to related information for treatment purposes, and offer to move to a more private setting for consultation if the patient requests.

F. WRITTEN COMMUNICATIONS

The rules apply to PHI in all forms such as electronic, written, verbal, and any other form.

1. Use of PHI in written medical records system: ACTCM staff, faculty and students are currently not using an electronic medical records system, so ACTCM uses handwritten medical intake forms and herbal prescription forms for medical treatment purposes. The Security Rule requires a number of physical steps to ensure that PHI contained in written form is protected:
    a. Clinic medical charts can only be accessed by clinic staff, faculty and students.
    b. The medical charts are stored behind the reception desk in metal cabinets that are locked each night, and patients and non-essential staff, faculty and students are restricted from the reception area.
    c. ACTCM Clinic has a dedicated file room that contains medical charts that is locked at all times.
    d. Charts are not left unattended and are not to leave the clinic area unless they are being used for a clinic theater class and faculty and students have received prior approval for use of the chart.
    e. Written charts and patients records stored at off-site clinics such as the ACTCM Ear Clinic, CIIS Ear Clinic, Women's Resource Center and GLIDE Clinic are not left unattended and are stored in a locked file cabinet and placed in a secure location at the end of each shift. Only authorized faculty, staff and students have access to the charts.

2. All written communications pertaining to the patient including records request, information billing information and written correspondence is stored within the patient's chart.

G. ELECTRONIC COMMUNICATIONS

The rules apply to PHI in all forms such as electronic, written, verbal, and any other form.

1. Use of PHI in electronic medical records system: ACTCM staff, faculty and students are currently not using an electronic medical records system, but ACTCM uses MediSoft software for accounting and billing purposes. The Security Rule requires a number of physical steps to ensure that PHI contained in computers is protected:
    a. MediSoft can only be accessed by clinic staff, each of which has a unique user name and password.
    b. The reception computers are turned off after business hours, and patients and non-essential staff, faculty and students are restricted from the computer area.
    c. ACTCM Clinic has a dedicated server located downstairs in a locked room.
    d. ACTCM Clinic computers are protected by a firewall and malware protection.
    e. ACTCM Clinic electronic files are backed up every night.
    f. MediSoft has audit controls to record and examine our records activities
    g. Controls are in place to ensure that health data has not been altered in an unauthorized manner
    h. Off-site clinics shifts located at CPMC and Berkeley Primary Care maintain electronic files according to those institutions own privacy policies and faculty and students receive appropriate training each semester.

2. Faxing: ACTCM's general policy is to mail PHI whenever possible. If faxing, only the PHI actually needed is sent and is only permitted if the sender first calls the recipient and confirms that the recipient or his or her designee will be waiting at the fax machine, and then calls the sender to confirm receipt of the document. Faxes may only be sent or received from the secure fax machine in the clinic reception area. The general fax machine on the first floor may not be used to fax or receive documents containing PHI.

    a. Each fax must use an ACTCM fax cover sheet containing the following confidentiality statement:

    Confidentiality Notice: This communication and any attachments are for the sole use of the intended recipient and may contain information that is confidential and privileged under state and federal privacy laws. If you received this fax in error, be aware that any unauthorized use, disclosure, copying, or distribution is strictly prohibited. If you have received this fax in error, please contact the sender immediately and destroy all copies of this message.

    b. If a fax containing PHI is transmitted to the wrong recipient:
        i. Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed.
        ii. Obtain written attestation that the recipient destroyed all copies and did not disclose the information
        iii. Fill out an incident report and submit it to the Privacy Officer.

2. Email: Emailing patient's PHI is discouraged, and do not send confidential information unless absolutely necessary.
    a. De-identify the information if possible

    b. Warn patients who communicate with email that their confidentiality cannot be ensured

    c. Add the following confidentiality notice footer to your message:

    Confidentiality Notice: This email communication and any attachments are for the sole use of the intended recipient and may contain information that is confidential and privileged under state and federal privacy laws. If you received this email in error, be aware that any unauthorized use, disclosure, copying or distribution is strictly prohibited. If you received this email in error, please contact the sender immediately and destroy/delete all copies of this message.

    d. If an email containing PHI is transmitted to the wrong recipient:
        i. Send an email to the incorrect recipient explaining that the information has been misdirected, and ask that the materials be returned or destroyed.
        ii. Obtain written attestation that the recipient destroyed all copies and did not disclose the information

iii. Fill out an incident report and submit it to the Privacy Officer.

H. DECEASED INDIVIDUALS

ACTCM must protect the PHI of deceased individuals to the immediate family in accordance with federal law. Such releases must be documented. ACTCM will retain all original PHI.

I. PERSONAL REPRESENTATIVES

ACTCM must treat an individual as the personal representative of a patient if the person is, under applicable state or other law, authorized to act on behalf of the patient in making decisions related to healthcare. However, the representative may receive PHI only to the extent to which the personal representative is authorized. In addition, the personal representative's rights are limited by the scope of his or her authority under state or other law.

V. LEGAL AND PUBLIC POLICY DISCLOSURES

The purpose of this policy is to explain the situations where a legal and public policy exception to the HIPAA rules allows ACTCM to use or disclose PHI without a written patient authorization or verbal permission, and to describe the relevant procedures ACTCM must follow when using or disclosing PHI in such situations.

A. RELEASE OF PHI FOR LEGAL AND PUBLIC POLICY PURPOSES

In many circumstances, ACTCM is allowed to use or disclose patient's PHI without the patient's explicit prior permission. ACTCM is allowed to use and disclose PHI for particular legal and public policy situations without obtaining any form of permission (i.e., authorization or verbal agreement) from the patient.

1. Specific situations where patient permission is not required. Listed below are separate categories of uses and disclosures for which ACTCM is not required to obtain affirmative permission from the patient prior to disclosure:

    a. Required by law: ACTCM may use or disclose PHI as required by law, if the use or disclosure complies with and is limited to the relevant requirements of such law.

    b. Public health activities: ACTCM may disclose PHI to a public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability (e.g., reporting communicable diseases), and the conduct of public health surveillance, investigations or interventions.

    c. Health oversight activities: ACTCM may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, investigations, inspections, licensure or disciplinary actions, civil, administrative, or criminal proceedings, or other activities necessary for the oversight of the health care system, government benefit programs, or civil rights laws. The ACTCM is permitted to

respond to a health oversight agency's request for PHI as well as initiate these disclosures on its own.

d. Judicial and administrative proceedings: ACTCM may disclose PHI in the course of a judicial or administrative proceeding if the request for PHI is made pursuant to a court or administrative order or in response to a subpoena or discovery request (or other lawful process) from a party to the proceeding. If the request is made pursuant to a court or administrative order, ACTCM may disclose the information requested without additional process. In such cases, ACTCM may disclose only the information expressly authorized by the order. Without a court order or subpoena issued by a court, ACTCM must take additional steps to ensure the confidentiality of the information before it is permitted to disclose the minimum PHI necessary to fulfill the request.

e. Law enforcement purposes: ACTCM may disclose PHI for law enforcement purposes to a law enforcement official under certain circumstances. Certain limited information may be disclosed to a law-enforcement official:
   i. As required by other law or court order, warrant, subpoena, or administrative request;
   ii. To identify or locate a suspect, fugitive, material witness, or missing person;
   iii. In response to a request about an individual who may be a victim of a crime;
   iv. About an individual who has died as a result of criminal conduct; or
   v. Where ACTCM believes that the information constitutes evidence of criminal conduct that occurred on the premises of ACTCM.

f. Specialized government functions: ACTCM may disclose the PHI of armed forces personnel if necessary for a military mission. ACTCM may also disclose PHI to federal officials for intelligence and national security activities, or to a law enforcement or correctional institution official who has custody of the individual and needs the information to provide health care to the individual or to protect the health and safety of others.

g. Workers' compensation: ACTCM may disclose PHI as necessary to comply with laws relating to workers' compensation or similar programs.

h. Serious threat to health or safety: ACTCM may disclose PHI if it believes in good faith that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is to a person reasonably able to prevent the threat, or is necessary for law enforcement authorities to identify or apprehend an individual.

B. VERIFICATION OF IDENTITY AND AUTHORITY

With the exception of disclosures made pursuant to valid authorizations, prior to disclosing PHI ACTCM must verify the identity of a person requesting the PHI and the authority of such person to access PHI requested, if the identity and/or authority is not known.

1. Conditions on disclosures: ACTCM must obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI that is a condition of disclosure under the privacy rules or other law.

2. Identity of public officials: ACTCM may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI 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 in writing, the request is on the appropriate government letterhead.

    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, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

3. Authority of public officials: ACTCM may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected 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, a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal.

VI. BUSINESS ASSOCIATES POLICY

This policy is to protect the privacy and confidentiality of PHI that ACTCM discloses to individuals and entities that are business associates of ACTCM. With the approval of the Privacy Officer or Clinic Director and in compliance with HIPAA, and ACTCM employee may disclose PHI to an approved ACTCM business associate.

A. GENERAL RULES REGARDING BUSINESS ASSOCIATES

The privacy rules define a business associate as a person or entity that provides certain functions, activities, or services to or for ACTCM, involving the use or disclosure of PHI. ACTCM may disclose PHI to a business associate, or allow the business associate to create or receive PHI on its behalf.

1. Limitations on the use of PHI: The business associate may only use the PHI that it receives in its capacity as ACTCM's business associate as permitted by law and its contract with ACTCM.

2. Additional compliance obligations: Disclosures of PHI to business associates must comply with all of ACTCM's other policies and procedures.

3. All individuals (employees, subcontracted employees, and volunteers) associated with ACTCM's business associate with access to PHI must sign ACTCM's Privacy and Confidentiality Agreement Form, and the signed Confidentiality Agreement Forms are placed in a secure binder located at the Privacy Officer's Desk.

B. IDENTIFICATION OF A BUSINESS ASSOCIATE

A business associate is a person or entity that:

1. On behalf of ACTCM, performs or assists in the performance of functions or activities involving the use or disclosure of PHI. Examples of such functions include but are not limited to:
    - Claims processing or administration
    - Data analysis, processing or administration
    - Utilization review
    - Quality assurance
    - Billing
    - Practice and records management

2. Provides the following services ACTCM where the provision of services involves the disclosure of PHI:
    - Legal
    - Actuarial
    - Accounting
    - Consulting
    - Data aggregation
    - Administrative
    - Accreditation

3. Provides services that impact areas where PHI is housed.
    - Janitorial services
    - Repair of equipment
    - Delivery of supplies and linen

C. AGREEMENTS WITH BUSINESS ASSOCIATES WITH ACCESS TO PHI

ACTCM staff and faculty must inform the Privacy Officer and/or the Clinic Director about all proposed agreements between ACTCM and an entity or individual, including an outside contractor, in which ACTCM will provide access to PHI. If it is uncertain whether the outside contractor will have access to PHI, he or she is instructed to forward the agreement to the Privacy Officer and/or Clinic Director for review.

D. Required Components of a Business Associate Agreement

A business associate contract must include provisions that:

1. Establish the permitted and required uses and disclosures of PHI by the business associate.

2. Prohibit other uses and disclosures by the business associate, except that the contract may permit the business associate to use and disclose PHI for the proper management and administration of its business and to provide data aggregation services for ACTCM.

3. Require appropriate safeguards to be implemented by the business associate to prevent inappropriate use or disclosure.

4. Ensure that agents and subcontractors of the business associate who receive PHI from ACTCM also agree to the same restrictions and requirements with regard to use and disclosure of the PHI.

5. Require the business associate to comply with HIPAA's requirement to allow individuals to review and copy their PHI.

6. Require the business associate to make available information that is required to provide an accounting of disclosures.

7. Require the business associate to make its internal practices, books, and records concerning PHI available to HHS.

8. Provide for the return or destruction of all PHI by the business associate at the termination of the contract.

9. Authorize ACTCM to terminate the contract if the business associate violates a material term of the contract.

E. Privacy Violations by a Business Associate

If Clinic staff, faculty or student knows or has reason to believe that a business associate of ACTCM is inappropriately using or disclosing PHI, whether the PHI was received by ACTCM or not, they are required to notify ACTCM's privacy officer immediately regarding the suspected violation.

1. Review of alleged violations: Upon receiving notice of an alleged or actual violation of a business associate agreement from any source, including notice obtained through patient complaints and incident reports, the Privacy Officer will initiate a review of the conduct or activities at issue.

2. Investigation and resolution of violations: If the Privacy Officer determines that the complaint, report or other form of notice contains substantial and credible evidence of

violations by a business associate, the Privacy Incident Response Team (PIRT) will commence a formal investigation into the conduct or activities of the business associate.

a. If the investigation reveals that a business associate has violated its agreement with ACTCM, the Privacy Officer shall notify legal counsel immediately.

b. If PIRT and/or legal counsel determine that the business associate has committed a material breach or violation of its obligations under the business associate agreement, the privacy officer, with the assistance of legal counsel, must take reasonable steps to remedy the breach or terminate the contract of a business associate when feasible

VII. MARKETING AND FUNDRAISING POLICY

All ACTCM marketing communications must comply with the HIPAA privacy rules' specific requirements as well as any applicable state law or regulations.

A. USE AND DISCLOSURE OF PHI FOR MARKETING

Use of PHI for marketing purposes as defined by HIPAA will require the patient's prior written authorization. While the majority of ACTCM's marketing communications do not involve financial remuneration, the Final Omnibus Rule further clarifies that if they do, patient authorization is required. All marketing projects conducted by CIIS/ACTCM's Communications or Foundation Department must comply with HIPAA and ACTCM's guidelines for use of PHI. Patients must have a clear way to opt-out of written or electronic communication, so the following statement should be included in all marketing communications:

If you do not wish to receive further marketing communications from ACTCM, please contact: ACTCM Clinic Privacy Officer, 455 Arkansas Street, San Francisco, CA 94107 or call 415-282-9603 or email ACTCMClinic@ciis.edu.

B. USE AND DISCLOSURE OF PHI FOR FUNDRAISING

Although HIPAA does not prohibit fundraising efforts that target patients, ACTCM uses only demographic information for fundraising communication. HIPAA specifies that all fundraising materials that target patients must include a clear way for the recipients to opt-out of future solicitations. The following statement should be included in all fundraising communications:

If you do not wish to receive further fundraising communications from ACTCM, please contact: ACTCM Clinic Privacy Officer, 455 Arkansas Street, San Francisco, CA 94107 or call 415-282-9603 or email ACTCMClinic@ciis.edu.

C. EXCEPTIONS TO THE GENERAL RULE

An ACTCM staff, faculty or student may use and disclose PHI without an authorization to make a marketing communication to a patient, if the communication:

1. Occurs in a face-to-face encounter with the patient; or

2. Concerns promotional gifts of nominal value provided by ACTCM (e.g., calendars, pens, and other general, inexpensive promotional merchandise and prizes).

D. CURRENT ACTCM MARKETING PROMOTIONS

ACTCM's Notice of Privacy Practice ("NPP") includes the following statement:

This office will not use your health information for marketing communications without your written authorization. However, this office may send birthday cards, miss you cards, thank you cards, event notifications, newsletters and appointment reminders, by telephone calls or mail.

E. FORMAT REQUIREMENTS

The authorization must conform in all respects with the requirements set forth in ACTCM's Authorizations Policy. In addition, if the marketing involves direct or indirect remuneration to ACTCM from a third party, the authorization must state that such remuneration is involved.

F. BUSINESS ASSOCIATES AND OTHER THIRD PARTIES

1. ACTCM's products or services: ACTCM may engage a business associate to conduct marketing activities on its behalf.
2. The third party's products or services: However, ACTCM may not sell or disclose PHI to a third party to help the third party market its own products or services without a signed authorization from the patient.

VIII. RIGHT TO ACCESS RECORDS POLICY

ACTCM shall process, in accordance with the procedures outlined below, a request to access, inspect, and/or obtain a copy of certain PHI maintained by ACTCM, if the request is made by a patient or his or her authorized representative.

A. RIGHT OF ACCESS TO PHI

In general, a patient has a right of access to inspect and obtain a copy of his or her PHI held by ACTCM, for as long as the PHI is maintained by ACTCM. Exceptions to the right of access are set forth below:

1. Written Requests: ACTCM requires the patient to make requests for access or copies in writing by submitting an ACTCM's Patient Records Request

2. Denials Without an Opportunity for Review: ACTCM may deny the patient's request for access without providing the patient an opportunity for review of the when the PHI was compiled by ACTCM in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

3. Denials with an Opportunity for Review: ACTCM may deny the patient access, so long as the patient is given a right to have the denial reviewed, if 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 the personal representative is reasonably likely to cause substantial harm to the patient or another person.

4. Right to Review of Denial: If ACTCM denies the patient access to his or her PHI, the patient has the right to have the denial reviewed by a member of PIRT to act as a reviewing official and who did not participate in the original decision to deny access. ACTCM must provide or deny access in accordance with the determination of that official.

5. Verification: Prior to disclosing PHI to a person unknown to ACTCM, ACTCM employees must verify the identity of the person requesting the PHI and the authority of the person to have access to the PHI requested. In addition, ACTCM must obtain any documentation, statements, or representations, whether oral or written, from the requestor when such information is a condition of the disclosure.

B. RESPONDING TO A REQUEST FOR ACCESS

If the information is maintained or accessible onsite, ACTCM must act on a request for access within 30 days of the date ACTCM received the request. If ACTCM cannot act on a request within the applicable deadline because the information is not maintained or accessible on-site, it may extend the deadline by no more than 30 days by providing the patient with a written statement of the reasons for the delay and the date by which ACTCM will complete its action on the request. ACTCM must provide the written statement within the original time period and may only extend the time period once.

1. Provision of access: If ACTCM grants a request for access, it must comply with the following requirements.
    a. ACTCM must notify the patient and provide the access as requested, including inspection or obtaining a copy, or both, of the PHI.
    b. ACTCM must provide the patient with access to the PHI in the form or format requested by the patient, if it is readily producible in this form or format; or if not, in a readable hard copy form or other form that is agreed upon by ACTCM and the patient.
    c. If acceptable to the patient and ACTCM, ACTCM may provide the patient with a summary or explanation of the PHI instead of providing access to the actual PHI.
    d. ACTCM must provide access in a timely manner, including arranging with the patient for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the patient's request.
    e. ACTCM may discuss the scope, format, and other aspects of the request for access with the patient as necessary to timely provide access.

f. If the patient requests a copy of the PHI or agrees to a summary or explanation, ACTCM may charge a reasonable cost-based fee, provided that the fee includes the cost of copying, postage, and preparing an explanation or summary of the PHI (if a summary is requested by the patient).

2. Denial of access: If ACTCM denies access to PHI, it must implement the following procedures:
   a. Give the individual access to any other PHI requested for which they are authorized to have access, to the extent possible, after excluding the PHI that ACTCM has grounds to deny access.
   b. Provide a timely, written denial to the patient. The denial must be in plain language and contain the basis for the denial; if applicable, a statement of the patient's right to review of the decision, including a description of how the patient can exercise these review rights; and a description of how the patient may complain to ACTCM or the Secretary of Health and Human Services, including the name or title and telephone number of the contact person or designated office.
   c. Inform the patient where to direct the request for access, if ACTCM does not maintain the PHI that is the subject of the patient's request for access, and ACTCM knows where the requested information is maintained.
   d. If the patient has requested a review of a denial, ACTCM must a member of PIRT who was not directly involved in the denial to review the decision to deny access. ACTCM must promptly refer the review request to the reviewing official. The reviewing official must determine, within a reasonable period of time, whether or not to deny access. ACTCM must promptly provide written notice to the patient of the reviewing official's decision and carry out the decision.

C. Documentation and Record Retention Requirements

ACTCM must document the records that are subject to access by patients and the titles of the persons or offices responsible for receiving and processing requests for access. ACTCM must retain this documentation for seven years from the date of its creation until seven years after the date when it was last in effect.

IX. REQUESTING AMENDMENTS POLICY

It is ACTCM's policy to respond to a patient's request for an amendment to his or her PHI held by ACTCM (and/or our business associates) in compliance with the HIPAA privacy rules.

A. Right to Amend Protected Health Information

A patient has the right to have ACTCM amend PHI about the patient that is contained in ACTCM's records for as long as the PHI is maintained by ACTCM.

1. Accepting a patient's request for amendment: If ACTCM has no grounds to deny the request for amendment ACTCM must do all of the following:

a. Make the appropriate amendment to the patient's PHI or record. ACTCM should, at a minimum, identify the records that are affected by the amendment and append or otherwise provide a link to the location of the amendment.
b. Inform the patient on a timely basis that the amendment is accepted and obtain the patient's identification of and agreement to have ACTCM notify the relevant persons with whom the amendment needs to be shared.
c. Make reasonable efforts to inform and provide the amendment within reasonable time to:
    i. Persons identified by the patient as having received PHI and needing the amendment, and
    ii. Persons, including business associates, that ACTCM knows have the unamended information and may have relied, or might rely in the future, on the information to the detriment of the patient.

2. Denying a patient's request for amendment: Under certain circumstances, ACTCM may deny the patient's request for amendment to his or her PHI held by the College for any of the following reasons:
    a. The PHI was not created by ACTCM, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
    b. The PHI is not part of the patient's designated record set.
    c. The PHI would not be available for inspection under ACTCM's policy regarding the patient's right to access to records.
    d. The PHI is accurate and complete.

3. Denial procedures: If ACTCM denies the requested amendment, in whole or in part, ACTCM must take the following steps:

    a. The ACTCM must provide the patient with a valid written denial that explains:
        i. The basis for the denial;
        ii. How the individual may file a written statement disagreeing with the denial;
        iii. The individual's options with respect to future disclosures of the disputed information; and
        iv. How the individual may make a complaint to HHS.

    b. ACTCM must permit the patient to submit to ACTCM a written statement disagreeing with the denial and the basis for the disagreement.

    c. ACTCM may prepare a written rebuttal to the patient's statement of disagreement.
        i. If ACTCM prepares a rebuttal, it must provide a copy to the patient.
        ii. ACTCM must identify, as appropriate, the information in the patient's record that is the subject of the disputed amendment and append or otherwise link to this information the patient's request for an amendment, ACTCM's denial of the request, the patient's statement of disagreement, and the ACTCM's rebuttal to the information.

d. ACTCM must adhere to the following guidelines if it makes future disclosures of the patient's disputed PHI:
    i. If the patient has submitted a statement of disagreement, ACTCM must include either the material appended to the record, or an accurate summary of it, with any subsequent disclosure of the PHI to which the disagreement relates.
    ii. If the patient has not submitted a written statement of disagreement, ACTCM has to include the appended information with any subsequent disclosure only if the patient has requested that ACTCM do so.

4. Time period for acting on requests: ACTCM must act on the patient's request for an amendment within 60 days of receipt of the request. If ACTCM is unable to act on the amendment within 60 days, however, ACTCM may extend the time period for 30 days, one time, so long as, within the original 60 day time limit, ACTCM provides the patient with a written statement of the reasons for the delay and the date by which ACTCM will complete its action on the request.

B. Documentation and Record Retention Requirements

ACTCM must document the titles of the persons or offices responsible for receiving and processing requests for amendments by patients. ACTCM must also document requests for amendments and the resolution of those requests. ACTCM must retain this documentation from the date of its creation until seven years after the date when it was last in effect.

X. ACCOUNTING OF DISCLOSURES POLICY

It is ACTCM's policy to provide patients, upon request, a timely accounting of certain disclosures of their PHI as required by law.

A. Right to an Accounting of Disclosures

The patient has a right to receive an accounting of all disclosures of his or her PHI made by ACTCM for the seven-year period prior to the date of the request.

1. Exceptions to the accounting requirement: ACTCM is not required to provide an accounting of disclosures that were made by the Clinic:
    a. For purposes of treatment of the patient;
    b. For payment activities, including billing, claims management, eligibility determinations, coordination of benefits, determination of cost-sharing amounts, and adjudication of health benefit claims;
    c. For health care operations, including management and administrative activities, patient service, quality assessment and improvement activities, training programs, auditing, compliance, business planning and development, and certain due diligence activities conducted in connection with the sale or transfer of assets;
    d. To the patient requesting the accounting;

e. To individuals involved in the patient's care where the patient verbally agreed to the disclosure;
f. To authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and certain other national security activities;
g. To a correctional institution or law enforcement official, upon a request by, and during such time as, the correctional institution or law enforcement official had lawful custody of the patient;
h. Incident to a use or disclosure that is otherwise permitted by the privacy rules; or
i. Pursuant to a valid patient authorization.

2. Suspension of accounting: A health oversight agency or law enforcement official may request that ACTCM temporarily suspend the patient's right to receive an accounting of disclosures to the health oversight agency or law enforcement official. Upon appropriate request, ACTCM must temporarily suspend a patient's right to receive an accounting of these disclosures for the time specified by such agency or official, if such agency or official provides ACTCM with a written statement that is an accounting to the patient would be reasonably likely to impede the agency's activities and specifies the time period for which such a suspension is required. But if that agency or official statement is made orally to ACTCM, ACTCM 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 30 days from the date of the verbal statement, unless a written statement from the agency or official is submitted during that time.

3. Time period for the response: ACTCM will act on a patient's request for an accounting no later than 60 days after receipt of such a request, in the following ways:
   a. ACTCM will provide the patient with the accounting requested; or
   b. If ACTCM is unable to provide the accounting within 60 days of receipt of the request, ACTCM may extend the time to provide the accounting once, by no more than 30 days, if ACTCM, within 60 days of receipt of the request, provides the patient with a written statement of the reasons for the delay and the date by which ACTCM will provide the accounting.

4. Fees for providing an accounting: ACTCM must provide the first accounting to a patient in any 12-month period without charge. ACTCM may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the same 12-month period. If a fee will be charged, ACTCM will inform the patient in advance of the fee and provide the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

B. Required Contents of an Accounting of Disclosures

An accounting of disclosures must be in writing and must contain the following elements for each disclosure:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI;
3. The address of the entity or person who received the PHI, if known;
4. A brief description of the PHI disclosed; and
5. Either a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure or a copy of a written request for a disclosure made pursuant to ACTCM's policy for disclosures to government entities.

C. RECORD RETENTION REQUIREMENTS

ACTCM must create and maintain the following documentation:

1. The core elements of each disclosure;
2. The written accounting that is provided to the patient;
3. The titles of the persons within ACTCM responsible for receiving and processing a patient's request for an accounting; and
4. The ACTCM must retain the required documentation for a period of seven years from the date of its creation, or the date when it was last in effect whichever is later.

XI. LAWS PERTAINING TO CLINIC PATIENT PRIVACY

A. OTHER FEDERAL LAWS

In addition to HIPAA, there are other federal laws which govern the release of information, mandate that information be protected, and in some cases require that individuals be granted certain rights relative to the control of and access to their information.

1. **Family Education Rights and Privacy Act (FERPA)**

The Family Education Rights and Privacy Act (FERPA) governs the protection of education records, which include student health records (20 USC 1232g). HIPAA specifically exempts individually identifiable health information in education records. As FERPA records are exempt from HIPAA, all releases from education records must be in accordance with FERPA regulations.

2. **Health Information Technology for Economic and Clinical Health Act (HITECH)**

The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 (42 CFR Parts 412, 413, 422 and 495, and 45 CFR Subtitle A Subchapter D) widened the scope of privacy and security protections required under HIPAA to address such things as business associate services and marketing activities, widened and increased the potential liabilities and consequences for non-compliance including civil and criminal penalties and fines, and provides for enhanced enforcement of the Privacy and Security Rules.

3. **Final Omnibus Rule**

The Final Omnibus Rule (45 CFR Parts 160 and 164) greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law. It implements a number of provisions of HITECH to strengthen the privacy and security protections for health information established under HIPAA.

It also extends responsibilities to Business Associates, clarifies self-pay restrictions, further defines marketing and fundraising activities, and more.

B. CALIFORNIA STATE LAWS

California has multiple statutes and regulations which require the protection of the privacy of its residents' confidential information such as credit cards, social security numbers, and personal identification numbers (PINs), as well as medical and insurance information. Major state privacy laws include:

1. California Health and Safety Code Section 1280.15

The California Health and Safety Code Section 1280.15 mandates that licensed facilities report any unlawful or unauthorized access, use, or disclosure of a patient's medical information no later than 5 business days after the breach has been detected. The institution is to report to both the Department of Public Health and the affected patient(s). See also California Health and Safety Code Section 130200.

2. California Information Practices Act (Civil Code Section 1798)

Codifies right to privacy as a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy of information pertaining to them; for example, names, social security numbers, physical description, home address, home telephone number, education, financial matters, and medical or employment history.

3. Confidentiality of Medical Information Act (CMIA)

Confidentiality of Medical Information Act (CMIA, Civil Code Section 56 *et seq*.) requires that:
• Confidentiality of medical information be protected and establishes the protections against disclosures of individually identifiable medical information
• Health care institutions notify California residents of breaches of electronic social security number, access codes to financial accounts, and medical and insurance information
• Health care institutions implement safeguards to protect the privacy and confidentiality of medical information and define personal liability for breaches of privacy.
These laws establish that individuals, not just institutions, are liable for any unauthorized access, use, disclosure, or viewing of medical information, and impose various civil penalties against an individual such as personal fines, civil liability, licensure sanctions, and/or criminal penalties. See also California Civil Code Sections 1785.11.2, 1798.29, and 1798.82.

4. Lanterman-Petris-Short Act (LPS)

The Lanterman-Petris-Short Act (LPS, Welfare and Institutions Code Section 5328 *et seq*.) provides special confidentiality protections for medical records containing mental health or developmental disabilities information.