

HIPAA Policies and Procedures

William T. Chen, MD, Inc.

General Rule 164.502

A Covered Entity may not use or disclose PHI except as permitted or required by the privacy regulations.

Permitted Disclosures:

1. To the individual
2. With a Consent, to carry out treatment, payment, or health-care operations.
3. Without consent, if in certain circumstances.
4. With an Authorization
5. As permitted and in compliance with the provisions permitting disclosures without consent, authorizations or opportunity to Agree or Object.

Required Disclosures:

1. To an individual, when requested as permitted and in compliance with the provisions permitting:
 - a. Access of individuals to PHI and
 - b. Accounting of disclosures of PHI.
2. When required by the Secretary to investigate or determine the Covered Entity's compliance.

Minimum Necessary 164.502(b)

When using or disclosing PHI or when requesting PHI from another covered Entity, a Covered Entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Minimum necessary does not apply to:

1. Disclosures to, or requests by, a health-care provider for treatment.
2. Uses or disclosures made to the individual.
3. Disclosures made to the Secretary of Investigations, Enforcement or Administrative Actions.
4. Uses for disclosures required by law.
5. Uses or disclosures required for compliance with the privacy regulations.

Uses and Disclosures of PHI Subject to an Agreed Upon Restriction 164.502(c)

A Covered Entity that has agreed to a restriction may not use or disclose the PHI covered by the restriction in violation of such restriction, except as otherwise provided.

Disclosures to Business Associates 164.502(e)

A Covered Entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf, if the Covered entity obtains written satisfactory assurance that the business associate will appropriately safeguard the information.

Deceased Individuals 164.502(f)

A Covered Entity must comply with the requirements of these regulations with respect to the PHI of a deceased individual.

Personal Representatives 164.502(g)

Except in a few limited circumstances, a Covered Entity must treat a personal representative as the individual under the privacy regulations.

Confidential Communications 164.502(h)

Covered entities must comply with requests for confidential treatment of communications as provided for in the privacy regulations.

Uses and Disclosures Consistent with Notice 164.502(i)

Uses and disclosures of PHI must be consistent with your Notice of Privacy Practices.

Disclosures by Whistleblowers and Workforce Member Crime Victims 164.502(j)

Workforce members and business associates may in good faith disclose PHI if the Covered Entity has engaged in:

1. Conduct that is unlawful or otherwise violates professional or clinical standards.
2. Or that the care, services, or conditions provided by the Covered Entity potentially endangers one or more patients, workers, or the public.

Disclosures by workforce members who are victims of crime:

Covered Entities may, with some limitations, disclose PHI if a member of its workforce, who is the victim of a criminal act, discloses PHI to a law enforcement official.

Business Associate Contracts 164.504

Business Associates with the office of William T. Chen, MD, Inc. must sign a Business Associate Contract. This contract will provide that the business associate will:

1. Not use or disclose PHI other than as required in the contract
2. Use appropriate safeguards to protect the information
3. Report any uses or disclosures not permitted
4. Ensure that their business associated are in compliance
5. Make the information available to the patient for inspection
6. Allow the patient to request an amendment
7. Provide an accounting of any non covered disclosures
8. Make its internal practices available to regulatory agencies
9. Agree to return or destroy all PHI upon termination of the contract, if feasible.

The office of William T. Chen, MD will keep an accurate listing of the office's contracts (oral and written). The Office Manager is responsible for contract drafting, negotiation and administration with the final decision being made by the Medical Director, William T. Chen, MD. All records shall be retained for a minimum of seven years.

Contracts with Business Associates can be **terminated** if the Covered Entity determines that the Business Associated has violated the terms of agreement as stated above and that the Business Associated demonstrated non-compliance with the HIPAA of 1996.

Obtaining Consent in Direct Treatment Relationship 164.506

Under specific conditions a provider may refuse to treat a patient who refuses to sign a consent form. In California, offices should obtain two forms of consent depending on the service being performed. They are the:

1. General consent to treat (HIPAA consent; and,
2. "Informed Consent" if the office intends to performs services that would be deemed invasive in nature.

The general consent need only be obtained once, as it will last the lifetime of the patient unless it is revoked in writing. Preferably, a general consent will be obtained at each procedure performed. To be valid, the general consent must inform the patient:

1. That PHI may be used or disclosed to carry out treatment, payment or health-care operations.
2. Of the offices' notice of privacy practices statement
3. Of the offices' right to change the privacy practices
4. Of the right to request restrictions
5. That the provider may not agree to the requested restrictions, but if the provider does agree, the restrictions are binding. Of the right to revoke consent in writing.
6. Must be signed and dated by the individual.

Both the general consent and the informed consent shall be a part of the patient's medical record with a copy of the consent given to the patient upon request. In an emergent situation, consent will be obtained by contacting the "emergency contact" in the PHI. If after three unsuccessful attempts to contact the "emergency contact", consent will be waived if the patients' life is in danger. Oral consent will be attempted and witnessed by an additional health-care worker.

The order of obtaining consent will be strictly adhered to but if conflicts or deficiencies do occur, the Privacy Officer and/or the Medical Director will investigate to determine if any privacy regulation has been compromised.

Consent not required in indirect Treatment Relationship 164.506(a)(2)

A health-care provider may, without consent, use or disclose PHI to carry out treatment, payment or health-care operations if the covered health-care provider has an indirect treatment relationship with the individual. Indirect treatment relationships generally refer to:

1. Pharmacies
2. Radiologist; and,
3. Laboratories

Joint Consents

Joint consents are permitted for Covered Entities that participate in an organized health-care arrangement.

A joint consent must:

1. Include the name or other specific identification of the Covered Entities, or

- classes of Covered Entities, to which the joint consent applies; and,
2. Meet the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the consent covers more than one Covered Entity.

Joints consents in this Covered Entity, William T. Chen MD, are not necessary as the Covered Entity is not part of and Organized Health-Care Arrangement.

Consent Revocation 164.506(b)(5)

An individual may revoke consent in writing at any time. Revocation will be effective except to the extent that the Covered Entity has already relied on the consent. Appropriate personnel both within and outside the organization shall be notified of the revocation as soon as possible.

If an individual revokes a joint consent, the Covered Entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as possible.

Revocation of consent shall be done in writing. The revocation shall be kept in the patient's chart with a separate listing of all revocations maintained in a separate file for easy access.

Consent Retention 164.506(b)(6)

In California, records must be retained a minimum period of seven (7) years.

The consent will be updated yearly or upon the next visit the individual has at the health-care provider's office. In the case where an individual has not been seen in the office for longer than 3 months, no information will be released until a new consent has been obtained by the health-care provider's office. The health-care provider's office will be responsible for maintaining and updating the consent form.

CA Welfare & Institution code 5326.2

Informed Consent

This is an additional California requirement and should be provided to a patient at the time that additional and invasive services are recommended. The Informed Consent must describe in a clear and explicit manner the following:

1. The reason for the treatment.
2. The nature of the procedure used.
3. The probable degree and duration of improvement or remission, expected with or without such treatment.
4. The nature, degree, duration, and the probability of the side effects and significant risks.
5. The reasonable alternative treatments and why the physician is recommending this particular treatment.
6. The patient's right to accept or refuse the proposed treatment, and that if the patient consents, has the right to revoke the consent for any reason, at any time prior to or between treatments.
7. The patient must sign and date the form.

A copy of the Informed Consent will be given to the patient with the original placed in the patient's chart.

See copy of Informed Consent in Procedure Manual.

Authorizations 164.508

Except as otherwise required or permitted by the privacy regulations, a Covered Entity must obtain an authorization to use or disclose PHI for purposes other than treatment, payment and healthcare operations.

CORE Elements of a valid authorization:

1. Is written in plain language.
2. Is dated and signed by the patient.
3. Includes a description of a person's authority to act on behalf of an individual if authorization is executed by a personal representative.
4. States the type of persons/entities authorized to disclose the information.
5. States the specific nature of information to be disclosed.
6. States the name or functions of the person or entities authorized to receive the information.
7. States the purpose for which the information is being collected.
8. Specifies the length of time the authorization shall remain valid.
9. Advises the person signing the authorization of the right to receive a copy of the authorization and the right to revoke an authorization.

Under HIPAA, there are only two reasons for obtaining an authorization:

1. To use PHI for anything other than treatment, payment or healthcare operations; or
2. To disclose PHI to an entity for anything not related to treatment, payment or healthcare operations.

In California, if you are a Covered Entity, you should obtain an authorization to use or disclose PHI from the patient at all times.

Treatment means the provision, coordination, or management of health care and related services by one or more healthcare providers, including the coordination or management of health care; consultation between healthcare providers; or the referral of a patient from one health-care provider to another.

Payment means the activities undertaken by a covered entity to obtain premiums, determine coverage and benefit responsibility or to obtain or provide reimbursement for provision of health care to an individual.

Healthcare operations shall refer to the any of the following activities if a Covered Entity or an organized healthcare arrangement in which the Covered Entity participates:

1. Conducting quality assessment and improvement activities;
2. Performing peer review, credentialing or other similar performance evaluations;
3. Performing underwriting, premium rate setting reinsurance and other risk related tasks;
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development including practice management and support; and,
6. Business management and general administrative activities of the covered entity, including, but not limited to:
 - a. Management activities relating to implementation of and compliance with the requirements of HIPAA;
 - b. Customer service functions;
 - c. Resolution of internal grievances;
 - d. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a Covered Entity or, following completion of the sale or transfer, will become a Covered Entity; and
 - e. Creating de-identified health information, fundraising and marketing for the Covered Entity.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within and entity that maintains such information.

Routine uses refer to disclosures made to:

1. State health agencies to report when patients have certain communicable diseases;
2. FDA to report information about medical devices that break or malfunction;
3. Child abuse or domestic violence agencies;
4. Police to investigate crimes;
5. Courts
6. Referring physicians
7. Labs
8. Pharmacies
9. Diagnostic imaging services

It is important in obtaining an authorization by a personal representative to find out before hand to which the patient divulges most often health information to and document the individual's name. Include in the process that the personal representative may be needed to sign an authorization on the patient's behalf and how the personal representative has this authority.

An authorization must be obtained to use or disclose the following information:

- a. Psychotherapy; or
- b. Genetic testing; or
- c. HIV; or
- d. Drugs/Alcohol

Psychotherapy Notes 164.508

Psychotherapy notes cannot be disclosed without prior patient authorization:

Except:

1. To carry out training programs in mental health under supervision; or
2. To defend a legal action or other proceeding brought by an individual.
3. Covered entities may also use and disclose psychotherapy notes without authorization in the following situations:
4. When required by the Secretary of DHHS to investigate compliance.
5. When required to do so by law.
6. When requested by a health oversight agency in order to oversee the originator of the notes.
7. To coroners regarding a deceased individual.
8. In order to prevent a serious and imminent threat.

Determine the difference between use and disclosure. Consent is needed for disclosure. Provide a Notice of Privacy practices for these services.

Authorization as Condition of Treatment 164.508(b)(4)

A Covered Entity may not condition the provision of treatment on the individual signing an authorization, except for the following:

1. A covered health care provider may condition the provision of research-related treatment (discussed below in section entitled Uses and Disclosure for Research that Includes Treatment).
2. A Covered Entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure.

A Refusal to treat based on unwillingness of a patient to sign an authorization must be:

- a. Limited to research-related treatment; or
- b. Limited to treatment provided solely for the purpose of creating protected health information for disclosure to third parties.

Consent of Authorizations Requested by a Covered Entity for its Own Used and Disclosures 164.508(c)

If a Covered Entity requests an authorization from the individual said authorization must contain the following elements:

1. A statement that the entity will not condition treatment on obtaining authorization from the individual except when those rules permit, including:
 - a. The provision of research-related treatment (see below); or
 - b. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of PHI to such third party.
2. A description of each purpose of the requested use or disclosure.
3. A statement that the individual may inspect or copy the PHI sought to be used or disclosed, and that the individual may refuse to sign the authorization.
4. A statement whether the use or disclosure will result in direct or indirect remuneration to the Covered Entity.

The authorization form shall include a place where the provider's office can initial or check that the individual has been given a copy of the signed authorization.

Content of Authorization for Uses and Disclosure for Research That Includes Treatment 164.508(f)

Unless waived by an Investigational Review Board (IRB) or privacy board, a Covered Entity that creates PHI for the purpose, in whole or in part, of research-related treatment must obtain an authorization for the use or disclosure of such information.

Such authorization must include the following elements:

1. A description of how PHI will be used or disclosed for treatment, payment or healthcare operations;
2. A description of PHI that may be disclosed without a consent, authorization or opportunity to agree or object.
3. When consent has been obtained and a notice of privacy practice has been given, a reference that acknowledges these actions and that they are binding;
4. A valid authorization may contain elements or information that are consistent with the requirements above.

A Covered Entity must provide the individual with a copy of the signed authorization.

Compound Authorizations: Combining Authorizations 164.508(f)

An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:

1. An authorization for use and disclosure of PHI for research that includes treatment may be combined with another authorization; or
2. An authorization for the use and disclosure of psychotherapy notes may be combined with other authorizations.

Authorizations and consents for all treatments and/or release of PHI shall remain separate. A copy of the consent and/or authorization shall be given to the individual before any treatment or release of PHI.

Revocation of Authorization. 164.508(b)(5)

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

1. The Covered Entity has taken action in reliance thereon; or
2. The authorization was obtained as a condition of obtaining insurance coverage.

A copy of the revocation of authorization shall be kept in both the patient's chart as well as in a "Revocations" file maintain by the privacy officer. All personnel involved shall be notified as soon as possible, either by fax for mail, of the revocation of authorization.

Opportunity for the Individual to agree of object 164.510

A provider may use or disclose PHI without obtaining consent or authorization if the individual is informed in advance and has the opportunity to object or restrict the disclosure.

The individual shall be notified in writing that the provider will be releasing PHI thirty (30) prior to release such information and that the individual shall notify the office within 10 days if there is an objection. The individual has the right to object without fear that there will be any negative repercussions.

Requirements for retaining effectiveness of prior consents and authorizations 164.532 (b)

A Covered Entity may use or disclose PHI in accordance with consents, authorizations or other legal permissions obtained before the compliance date of the privacy regulations (collectively "previous consent").

Any use or disclosure must comply with the terms of the previous consent, and use or disclosure for purposes other than treatment, payment of health care operations must be specifically permitted by the previous consent.

A consent form must be on file if a family member is involved in the patient's care, unless the patient is under 18 years of age, not capable of handling their personal and medical needs due to extreme illness, mental retardation or court

order. A copy shall be given to the patient and shall be noted on the record that a family member is in charge of care for this patient unless consent is revoked.

A record of what was released to the family member in charge of patient care and treatment shall be maintained in the patient's file.

A revocation of consent in writing is needed when the patient decides he no longer wants a family member involved in his care or treatment. Revocation of consent shall be kept in the patient's chart as well as in the "Revocation" file maintained by the privacy officer.

Uses and Disclosures Without Individual Consent, Authorization or Opportunity to Object or Agree. 164.512

A Covered Entity may use or disclose PHI without the individuals prior consent or authorization in the following situations:

1. California law requires disclosure.
2. By court order
3. To a government entity.
4. By civil or criminal subpoena
5. By warrant
6. To patient or their representative
7. To a coroner.

Records shall be maintained on all cases where PHI was released due to the above reasons.

PHI shall also be disclosed in the following situation:

1. Abuse, neglect or domestic violence;
2. For judicial and administrative proceedings, law enforcement purposes;
3. Regarding the death of a patient;
4. For transplants;
5. For research purposes;
6. To prevent or lessen a serious or imminent threat to the health or safety of a person or the public;
7. For worker's compensation
8. For other specialized government functions.

De-identification of PHI 164.514

Information is de-identified if the following is eliminated from the information being disclosed:

1. Name;
2. All geographic subdivisions smaller than a state;
3. All elements of dates (except for year, directly related to the patient);
4. Telephone numbers;
5. Fax numbers;
6. Email address(es);
7. Social Security Number;
8. Medical records number;
9. Health plan beneficiary number;
10. Account number;
11. Certificate or license number;
12. Vehicle identifiers and serial numbers;
13. Device identifiers and serial numbers;
14. URL's
15. ISP address numbers;
16. Biometric identifiers, including voice and finger prints;
17. Full face photographic images or any other comparable images;
18. Any other unique identifying number, characteristic, codes.

All information, which may lead to identifying an individual, must be removed before the information can be used or disclosed without prior consent. If in question, consent must be obtained.

Minimum Necessary Requirements 164.502 (b)(1)

Covered entities must make reasonable efforts to limit the disclosure of or request for PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request.

Exceptions: The minimum necessary rule does not apply to:

1. Disclosures to or requests by a health care provider for treatment;
2. Disclosures to individuals regarding to whom the PHI pertains;
3. Disclosures made under an authorization requested by an individual;
4. Disclosures made to the Secretary of DHHS for HIPAA compliance and enforcement efforts;
5. Uses or disclosures that are required by law; or
6. Uses and disclosures that are required for compliance with the HIPAA privacy standards.

When the minimum necessary rule applies, a Covered Entity may not use, disclose, or request an entire medical record unless it is specifically justified as the amount reasonably necessary to accomplish the purpose.

Minimum necessary refers to the minimal amount of information needed to obtain the background information to make professional decisions on health care. Disclosures for purposes of treatment are not subject to the minimum necessary standard, the entire medical record may be disclosed to another provider for purposes of treatment.

Uses and Disclosures of PHI for Marketing 164.514(e)(3)

A Covered Entity may not use or disclose PHI for marketing without the authorization except if the marketing:

1. Occurs in a face-to-face encounter;
2. Concerns products or services of nominal value; or
3. Concerns the health-related products and services of the provider;
4. Identifies the covered entity that is making the communication;
5. States whether the covered entity is being compensated for making the communication; and
6. Tells the patient how to opt out of further marketing communications; and
7. Explains why the patient is being targeted

For all other communications that are “marketing”, the covered entity must obtain the patient’s authorization to use or disclose PHI to create or make the marketing communication.

Marketing means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. It does not include communicating with participating providers or plans in a network or describing the services offered by a provider or benefits covered by the health plan.

Uses and Disclosures for Fundraising 164.514(f)(1)

The following information may be used without authorization to support fundraising efforts:

1. Demographic information relating to an individual; and
2. Date of health care provided to an individual.

Fundraising Requirements 164.514 (f)(2)

Notice of Privacy Practices. Covered entities must include their intention to use PHI in fundraising activities in their notice of privacy practices.

Opt Out Right. Fundraising materials must provide an opportunity for the recipient to opt-out.

The Covered Entity must make reasonable efforts to ensure that individuals who decide to opt out are not sent fundraising communications.

If an individual wants to opt-out for marketing purposes, their mailing address shall be removed from the database to ensure that no mailings are sent to them. Their account will also be flagged to ensure privacy.

Verification Requirements 164.514(h)(1)

Prior to any disclosures, a Covered Entity must:

1. Verify the identify of the person requesting PHI, as well as the authority of that person to have access to PHI; and,
2. Obtains documentation defining the nature of the request from the person requesting the PHI.

Healthcare providers are required to verify the identity of the person requesting the PHI and the authority of this person to have access to the protected health information. Written verification by the individual on the record is necessary before any information can be given out. Failure of the employee to do so could result in negative consequences not only for the employee but for the health care provider as well.

Notice of Privacy Practices 164.520

An individual has the right to adequate notice of a Covered Entity's uses and disclosures of his or her PHI, and the individual's rights and the Covered Entity's legal duties with respect to PHI.

Your notice must contain a header and the following information:

1. At least one example of how information is used and one example of how information is disclosed;
2. A description of the reasons for disclosure;
3. Prohibited used and disclosures;
4. A separate statement for specific types of disclosures;

5. A statement of the patient's rights;
6. A statement of the covered entities duties;
7. An explanation of the patient's right to complain and to whom they may file the complaint;
8. The name and contact information of the Privacy Official; and
9. The effective date of the notice.

The health care provider must provide this notice no later than the first date of treatment. Each patient will receive this written notice on the date of his or her next appointment or whenever he or she returns to the health care provider's office for a follow-up visit. No information will be released without the written consent of the patient or patient's representative.

If revisions of the privacy notice are necessary, these revisions will be distributed to all patients on their next office visit if it has been determined that their original notice did not contain the updated information. No information will be used or disclosed until the patient has signed the update privacy notice.

Right to Request Restrictions of Uses and Disclosures 164.522(a)

A Covered Entity must allow individuals to request restrictions on the use and disclosure of their PHI, although the Covered Entity may deny an individual's request or limit the scope of such restriction if it believes the restriction is not in the individual's best interests.

If the Covered Entity agrees to such restrictions, the Covered Entity must document and abide by the restrictions.

The restrictions that this office will agree to abide by will be evaluated on a case by case basis. It is important to recognize that each person has the right to request restrictions even if the office does not agree to such restrictions.

The individual shall be notified in writing that his/her requested restrictions cannot be adhered to after careful consideration. This information shall be part of their medical record. The termination of restrictions refers to PHI after the individual has been informed. The patient does have the right to confer with the privacy official and Medical Director to discuss the issue.

Business associates shall also be notified of the termination of restrictions on PHI.

Terminating a Restriction 164.522(a)(2)

A Covered Entity may terminate its agreement to a restriction, if:

1. The individual agrees to or requests the termination in writing,
2. The individual orally agrees to the termination and the oral agreement is documented; or,
3. A Covered Entity informs the individual it is terminating an agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has informed the individual.

Right to Request Confidentiality in Communications 164.522(b) (1)

A Covered Entity must permit individuals to request and must accommodate reasonable request by the individuals to receive communications of PHI from the Covered Entity by alternative means or at alternative locations.

A Covered Entity may require that the request:

1. Is reasonable with respect to the administrative burden;
2. Is in writing; and
3. Specifies an alternative address or other method of contact, and that (where relevant) the individual provides information on how payments should be handled.

Access of individuals to PHI (Protected Health Information) 164.524

An individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set.

Exceptions:

1. Psychotherapy;
2. Information obtained for purposes of litigation;
3. Information related to the Clinical Laboratory Improvements Amendment.

Some grounds for denial include:

1. Disclosure will likely endanger the patient; or
2. Disclosure would reasonably likely cause substantial harm to another person.

If access is requested by authorization, the office may charge a reasonable administrative fee of no more than \$16.00 per hour per person and .10 cents per page.

If access is requested by authorization through an attorney or their representative, the only administrative fee shall be \$15.00 plus the reasonable cost to retrieve the records.

If access is requested by subpoena, the office may charge an administrative fee of no more than \$24.00 per hour per person and .10 cents per page.

Response for requests for records must be done within 30 days and one extension may be requested for an additional 30 days.

If access to a patient's record is denied, the Medical Director shall be the reviewing official to determine if the denial is justified. The review process will take no longer than 30 days at which time the individual will receive a written response from the Medical Director.

If it is determined that the patient should not have been denied access, then the patient will be allowed to view the live medical record in the office of the health care provider. A copy of the record can be provided to the patient for a fee of \$15.00 or .10 cents per page. A log shall be maintained as to the date and to whom a copy of the record was given.

Amendment of Protected Health Information 164.526

An individual has the right to request an amendment to PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

California law requires that the health care provider allow any adult who inspects the record to write an addendum to the record. The health care provider is required to attach the addendum to the patient's records and include the addendum in any future disclosure.

1. All addenda must not exceed 250 words.
2. You must act or respond to the request within 60 days of receipt of the request and are allowed one 30 day extension, which must be requested by the provider and granted by the requestee.

This is based on California law and supersedes the HIPAA requirement. All Covered Entities shall be notified of the addendum. The privacy official of the health care provider shall be the person in charge of receiving and processing requests for each addenda by the patient.

Accounting of Disclosures of Protected Health Information 164.528

An individual has a right to receive an accounting of disclosures of PHI by the Covered Entity.

The exceptions are:

1. Disclosures to carry out treatment, payment and healthcare questions;
2. Disclosures to an individual who is not the subject of the PHI;
3. Disclosures in facility directories;
4. Disclosures for national security purposes;
5. Disclosures to correctional institutions or for law enforcement purposes; and,
6. Disclosures that occurred prior to the compliance date.

The health care provider's office must act within 60 days and is allowed one 30-day extension upon prior notification.

If an individual requests from a health care provider's office an accounting of disclosures of PHI, the office has up to 30 days to respond and all efforts will be made to facilitate this in a timely fashion. It shall be documented and logged that the accounting was provided to the individual on a particular date. The privacy official shall be responsible for receiving and processing requests for accounting by a patient or their representative.

Administrative Requirements 164.530

As a Covered Entity, the health care provider's office is required to:

1. Designate a Privacy Official, in writing.
2. Train staff regarding privacy.
3. Provide for staff's safety and protection
4. Protect the privacy of our patient's PHI.
5. Establish a procedure for complaints.
6. Discipline any wrongful use or disclosure of PHI.
7. Attempt to reduce any harmful effects cause by a wrongful use or disclosure.
8. Not harass or intimidate whistleblowers.
9. Standardize, whenever possible, policies and procedures.

Privacy Official 164.530 (a)

A Covered Entity is required to designate:

1. A Privacy Official, responsible for the implementation and development of the Covered Entity's privacy policies and procedures; and

2. A contact person or office that is responsible for receiving complaints about privacy violation who is able to provide further information about matters in the privacy notice.

The Privacy Official shall be the Office Manager. All complaints regarding violations of HIPAA shall be reported to her.

Training

A Covered Entity must establish appropriate training programs for the workforce. Training classes must be held annually and documented in the employee's file. Employees will be mandated to review and sign a confidentiality form that informs them of the patient's right to privacy and HIPAA rules and regulations.

Safeguards 164.530 (c)

A Covered Entity must establish appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

Locks shall be available on all cabinets, drawers or room doors that store patient information. For protection of the workforce, the door from the patient wait area to the rooms where the patient sees the physician shall be locked. Patient information shall be available to all personnel, Office Manager, Clinical Specialists but unavailable to part-time employees whose jobs do not depend on knowing any personal health information on patients.

Complaints 164.530 (d)

A Covered Entity must provide a process for individuals to make complaints concerning the Covered Entity's policies and procedures required by this subpart or its compliance with such policies and procedures.

Individuals may file complaints concerning the Covered Entities policies and procedures. The complaint must be made in writing and submitted to the privacy officer. There is no limit on the number of complaints an individual files. All complaints will be maintained in the patient's chart as well as a copy maintained in the complaint log with the privacy official. Disposition of the complaint shall be documented also.

Sanctions 164.530 (e)

A Covered Entity must establish and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the Covered Entity, except disclosures by whistleblowers and workforce member crime victims.

Members of the workforce are bound to keep PHI private and will face discipline action by the employer if policies and procedures are not carried. Depending on the severity of the use or disclosure, employment can be suspended or terminated. The Medical Director of the health care facility will determine the extent of the sanction,

Patient records shall be randomly audited semi-annually to ensure that policies and procedures on privacy are being properly handled and maintained. This information will be presented to the Medical Director for follow up.

Mitigation 164.530 (f)

In the event a wrongful use or disclosure occurs, the office must attempt, to the extent possible, mitigate the harmful effects of the wrongful use or disclosure. The privacy official must notify the patient and Medical Director of the breach in security and the Medical Director and privacy official must try to determine the depth of the breach and its effect on the patient.

Whistleblower 164.530 (g)

The health care provider's office may not retaliate against a member of its workforce if an individual notifies or complains to the proper authorities of any potential violations of these regulations.

Anyone within the workforce or outside has the right to file a complaint and to be free from intimidation, threat, coercion, discrimination or any other retaliatory act. The privacy official shall be the person who will be responsible for receiving and investigating the complaint regarding privacy.

Policies and Procedures 164.530

The health care provider's office is required to write and implement policies and procedures that are designed to comply with HIPAA and State privacy and confidentiality regulations.

Documentation 164.530 (l)

A Covered Entity must maintain its policies and procedures discussed in 164.530 (l), communications and actions and designations required by these regulations in written or electronic form for six years from the date of its creation or the date when it was last in effect, whichever is later.