

EXECUTIVE SUMMARY – HIPAA PRIVACY REGS FOR GROUP HEALTH PLANS

GENERAL RULES ON USES AND DISCLOSURES

A covered entity cannot use or disclose protected health information, except as follows:

- To the individual that is the subject of the information;
- For group health plans, unless consent has been sought as part of the enrollment process, without consent for purposes of treatment, payment and health care operations;
- As stated in a signed authorization from the individual. Required for use and disclosure of psychotherapy notes.

Minimum Necessary Rule

In requesting or disclosing protected health information, a covered entity is required to limit the information requested or provided to the minimum necessary to complete the intended use of the request or disclosure.

De-Identified Health Information

Use and disclosure of de-identified information is not subject to the regulation, provided it meets the regulations requirements for being de-identified.

BUSINESS ASSOCIATES

Protected health information may be disclosed to a business associate by a covered entity or received by a business associate on behalf of the covered entity, if satisfactory assurance that the business associate will safeguard the information is obtained in the form a written contract or agreement between the covered entity and the business associate.

PRIVACY NOTICE

A covered entity that creates or receives protected health information is required to provide notice to affected individuals of the uses and disclosures that may be made, and of the individual's rights regarding their protected health information and the covered entity's legal obligations. In the case of a group health plan, the notice must be provided by:

- For a self funded, group health plan, the employer sponsoring the plan;
- For a fully insured, group health plan, the insurance company or HMO issuing the coverage. Note if the employer receives protected health information, other than summary information or information on enrollment/termination, the employer is required to maintain a privacy notice and provide it upon request to any individual.

If a covered entity maintains a web site that provides information about the covered entity's customer services or benefits, it must prominently post its Privacy Notice on the web site and make it available electronically through the web site.

DISCLOSURE OF PROTECTED HEALTH INFORMATION TO THE PLAN SPONSOR

In order for the employer that sponsors a group health plan to receive protected health information, the self funded plan or insurer must receive verification that the plan documents have been amended to restrict uses and disclosures by the employer. In the case of a fully insured plan, this requirement does not apply to the provision of summary health information for the purposes of obtaining premium quotes, or modifying or terminating the plan or to enrollment or termination information.

Disclosures to the employer must be limited to those necessary to carry out plan administration functions that the employer performs and may not be made unless a statement is included in the appropriate Privacy Notice regarding the employer's receipt of such information.

CONSENTS

A group health plan is not required to obtain a consent prior to using or disclosing protected health information for the purposes of treatment, payment or health care operations.

AUTHORIZATIONS

An authorization is required for any use or disclosure of protected health information other than:

- Disclosures to the individual that is the subject of the information;
- For group health plans, for purposes of treatment, payment and health care operations.

INDIVIDUAL'S RIGHT TO REQUEST RESTRICTIONS ON USES AND DISCLOSURES

A covered entity is required to allow an individual to request that the covered entity restrict its uses and disclosures of protected health information. A covered entity is not required to agree to a requested restriction.

INDIVIDUAL'S RIGHT TO AMEND PROTECTED HEALTH INFORMATION

A covered entity must amend, at the request of the individual, protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in a designated record set.

ACCOUNTING OF DISCLOSURES

A covered entity is not required to provide an accounting of the following types of disclosures, as allowed under the regulation:

- Disclosures to carry out treatment, payment and health care operations;
- Disclosures made to the individual that is the subject of the information;
- Disclosures made under a signed authorization from the individual.

REQUIREMENTS FOR COVERED ENTITIES

Except for requirements relating to the prohibition of retaliatory acts and the prohibition of requiring waiver of rights under the regulation, a group health plan that is fully insured and receives only summary health information and information on enrollment and termination is not subject to the requirements for covered entities.

Covered entities, including self funded group health plans, are required to:

- Designate a Privacy Officer who is responsible for developing policies and procedures necessary for compliance with the regulation;
- Designate a contact person or office that is responsible for receiving complaints and providing information regarding the Notice of Privacy Practices;
- Provide training regarding privacy policies and procedures to all employees, if necessary or appropriate for the employee to be able to do their job.
- Put in place reasonable and appropriate administrative, technical and physical safeguards to prevent the, intentional or unintentional, use or disclosure of protected health information in violation of the regulation;
- Provide a process for individuals to file complaints;
- Put in place and apply appropriate sanctions for employees who fail to comply with privacy policies and procedures of the covered entity or who violate the regulation;
- Mitigate, to the extent practical, any harmful effect that is known to the covered entity and resulted from the use or disclosure of protected health information by the covered entity or its business associates;
- Not discriminate against or take retaliatory action against an individual who exercises their rights under the regulation;
- Implement policies and procedures that are reasonably designed to comply with the requirements of the regulation, taking into account the size and activities of the covered entity.

HIPAA PRIVACY REGS

(Eff. Date 4/14/03 or 4/14/04 for Small Health Plans)

The Health Insurance Portability and Accountability Act of 1996 contained provisions requiring the Department of Health and Human Services (HHS) to release regulations implementing the privacy requirements of the Act, if Congress did not enact legislation to implement them. On December 28, 2000, HHS released the final Privacy Regulations. Final modifications to the Privacy Regulations were released on August 14, 2002.

The Privacy Regulations apply directly to health plans, health care clearinghouses, and health care providers if that provider transmits any health information in an electronic format. The regulations apply indirectly to all business associates of a covered health plan, health care clearinghouse or health care provider by requiring these covered entities to include a compliance statement in the contract with any business associate.

A copy of the Privacy Regulation and the Final Modifications to the Privacy Regulation can be downloaded from the Internet at <http://www.hhs.gov/ocr/hipaa/finalreg.html>. Section number references from the regulation have been provided below to assist you in finding the provisions in the regulation for more detail.

DEFINITIONS

Business Associate. A person or entity that performs on behalf of, or assists, a covered entity in a function or activity involving the use or disclosure of individually identifiable health information. This includes standard functions normally performed by a TPA, UR Company, or Network; as well as other services provided to a covered entity such as legal, actuarial, accounting, consulting, data aggregation, and financial services. (*§160.103 - Definitions*)

Covered Entity. A health plan, a health care clearinghouse; a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Act. (*§160.103 - Definitions*)

Designated Record Set. A group of records maintained by or for a covered entity that consists of the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan. (*§164.501 - Definitions*)

Disclosure. The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. (*§164.501 - Definitions*)

Group Health Plan. An employee welfare benefit plan, as defined in ERISA, including insured and self-insured plans, to the extent that the plan provides medical care or coverage to employees or their dependents, and has 50 or more participants or is administered by an entity other than the employer that sponsors the plan. (*§160.103 - Definitions*)

Health Care Clearinghouse. A public or private entity, including a billing service, repricing company, and “value-added” networks, that processes or facilitates the processing of health information received in a non-standard format or containing non-standard data content into standard data elements or a standard transaction; or receives a standard transaction and processes or facilitates the processing of health information into non-standard format or non-standard data content. (*§160.103 - Definitions*)

Health Care Operations. Any of the following activities performed by or behalf of a covered entity:

- Quality assessment, protocol development, case management, provision of information about treatment alternatives;
- Evaluation of provider or health plan performance;
- Underwriting, premium rating, and other activities relating to the placement of a contract of health insurance or health benefits, including obtaining reinsurance, stop-loss/excess loss insurance for the plan;
- Conducting or arranging for medical review, legal services, and auditing functions;
- Business planning and development, such as conducting cost-management and planning-related analyses; and

Business management and general administrative activities of the entity.
(§164.501 - Definitions)

Marketing. To make a communication about a product or service a purpose of which is to encourage the purchase or use the product or service. Provided that there is not any direct or indirect payment from a third party, marketing does not include communications to describe a health related service or product provided or included in a plan of benefits, or communications made in the course of managing the treatment of that individual, or communications for the purpose of recommending to that individual alternative treatments, therapies, health care providers, or settings of care.
(§164.501 - Definitions)

Protected Health Information. Information, that identifies the individual or could reasonably be used to identify the individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. This includes information that is transmitted or maintained in any form or medium, electronic or otherwise. Information obtained and held by a covered entity in their role as an employer is not protected health information. (§164.501 - Definition of Individually Identifiable Health Information and Definition of Protected Health Information)

Small Health Plan. A health plan with annual receipts of \$5 million or less. (§160.103 - Definitions)

Summary Health Information. Information that may be individually identifiable health information and that summarizes history, expense or type of claims incurred by individuals covered by the group health plan. Such information must meet the requirements of being de-identified, as stated below, except that aggregation is allowed to the 5 digit zip-code. (§164.504(a) - Definitions)

PRIVACY RULE

General Rules on Uses and Disclosures

A covered entity cannot use or disclose protected health information, except as follows:

- To the individual that is the subject of the information;
- For health care providers, for purposes of treatment, payment and health care operations;
- For group health plans, unless consent has been sought as part of the enrollment process, without consent for purposes of treatment, payment and health care operations. If consent has been sought as part of the enrollment process, disclosures for treatment, payment and health care operations require a signed consent from the individual;
- As stated in a signed authorization from the individual. Required for use and disclosure of psychotherapy notes.
- Without authorization, consent, or the opportunity to agree for the following:
 - Disclosures required by law
 - Disclosures related to public health activities
 - Disclosures to a health oversight agency in relation to oversight activities of that agency
 - Disclosures required as part of a judicial or administrative hearing
 - Disclosures for law enforcement purposes
 - Disclosures to comply with laws relating to workers' compensation or other similar programs established by law.
- Disclosures that are incidental to a use or disclosure otherwise allowed under the regulation.

(§164.502(a) - General Rules)

Except for disclosures that only require the opportunity to agree, the covered entity must verify the identity of a person requesting protected health information and their authority to have access to the information, if the person or authority is not known. The covered entity must also obtain any documentation, written or oral, that is required by the regulation to provide the disclosure (e.g. consent, authorization, agreement to disclosure).

(§164.514(h) - Verification Requirements)

Personal Representatives

In the following circumstances, a covered entity must treat a personal representative of the individual as if they were the individual for purposes of complying with the regulation:

- Under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor;
- Under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor;
- Under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate.

(§164.502(g) - Personal Representatives)

Minimum Necessary Rule

In requesting or disclosing protected health information, a covered entity is required to limit the information requested or provided to the minimum necessary to complete the intended use of the request or disclosure. This rule does not apply to disclosures or requests made to the individual the information is about, made by the Secretary of Health and Human Services, or that are required by law.

(§164.502(b) - Minimum Necessary)

A covered entity must identify the members or job classes in its workforce that need access to protected health information, the type of protected health information necessary to carry out their duties, and then make reasonable efforts to limit their access to protected health information to the minimum necessary.

For routine and recurring disclosures, a covered entity must implement policies and procedures that limit the protected health information disclosed to the minimum necessary to achieve the purpose of the disclosure. For all other disclosures, the covered entity must review the request individually and develop criteria to limit the disclosure to the minimum necessary.

A covered entity can rely on a requested disclosure being the minimum necessary when the request is made by:

- Public officials, if the public official indicates it is the minimum necessary;
- Another covered entity;
- A business associate who is providing professional services to the covered entity.

(§164.514(d) - Minimum Necessary Requirements)

De-Identified Health Information

A covered entity can use protected health information, or disclose it to a business associate, for the purpose of creating information or data that is no longer individually identifiable. The regulation does not require that the de-identified information be for the covered entity's use.

Use and disclosure of de-identified information is not subject to the regulation, provided it meets the regulations requirements for being de-identified.

(§164.502(d) - Uses and Disclosures of De-Identified Protected Health Information)

A covered entity may determine that health information is de-identified only if:

- A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used to identify an individual and the methods and results of the analysis are documented; or

- ❑ The following identifiers have been removed: names; geographic subdivisions smaller than a State, except for the initial three digits of a zip code; all elements of dates (except year) for dates directly related to an individual; telephone numbers; fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers; device identifiers and serial numbers; web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers; full face photographic images; and any other unique identifying number, characteristic, or code.
(§164.514(b) - Requirements for De-Identification)

Limited Data Set

A covered entity can use or disclose a limited data set of protected health information only for the purposes of research, public health and health care operations. The regulation does not require that the limited data set be for the covered entity's use and allows for disclosure of protected health information to a business associate for the purpose of creating a limited data set.

Use and disclosure of a limited data set is subject to the regulation which requires that a written Data Use Agreement be in place prior to making any disclosure of a limited data set. A Data Use Agreement is required to contain, at a minimum, the specific provisions outlined in the regulation, which are similar in nature to that of a Business Associate Agreement.

A limited data set is similar in nature to de-identified health information, except that the following three elements may be included in a limited data set that are not allowed in de-identified data: City, State and zip code; dates that directly relate to the individual; and miscellaneous identifiers or codes.
(§164.514(e) - Requirements for De-Identification)

BUSINESS ASSOCIATES

Protected health information may be disclosed to a business associate by a covered entity or received by a business associate on behalf of the covered entity, if satisfactory assurance that the business associate will safeguard the information is obtained in the form a written contract or agreement between the covered entity and the business associate.
(§164.502(e) - Disclosures to Business Associates)

A Business Associate Agreement is required to contain, at a minimum, the specific provisions outlined in the regulation. Attachment 1 - Business Associate Agreements includes a listing of the required provisions.
(§164.504(e)(2) - Business Associate Contracts)

If a covered entity knows of an activity or practice of a business associate that represents a breach of the business associate's agreement, the covered entity is required to take reasonable steps to end the activity or practice and if that is not successful, terminate the agreement with the business associate. If it is not possible to terminate the agreement, the covered entity is required to report the business associate to the Secretary of Health and Human Services.
(§164.504(e)(1) - Business Associate Contracts)

For all covered entities, other than a small health plan, if prior to the date of compliance with the regulation the covered entity has written contracts in place with a business associate, the covered entity will not have to modify the that contract to comply with the requirements of a Business Associate Agreement until the earlier of the first renewal or modification of the contract or April 14, 2004.
(§164.532(e)(2) - Limited Deemed Compliance Period)

PRIVACY NOTICE

A covered entity that creates or receives protected health information is required to provide notice to affected individuals of the uses and disclosures that may be made, and of the individual's rights regarding their protected health information and the covered entity's legal obligations. In the case of a group health plan, the notice must be provided by:

- For a self funded, group health plan, the employer sponsoring the plan;
- For a fully insured, group health plan, the insurance company or HMO issuing the coverage. Note if the employer receives protected health information, other than summary information or information on enrollment/termination, the employer is required to maintain a privacy notice and provide it upon request to any individual.

A covered entity that is required to maintain a Privacy Notice is prohibited from using or disclosing protected health information in a manner that violates the Notice.

(§164.520(a) - Notice of Privacy Practices, §164.502(i) - Uses and Disclosures Consistent with Notice)

A group health plan or insurance company that is required to provide a Privacy Notice must provide notice to the covered employee at the following times:

- By the compliance date for the health plan, for all individuals covered by the plan at that time;
- At the time of enrollment, for each new enrollee; and
- Within 60 days of a material revision to the notice, for all individuals covered by the plan at that time.

In addition, a group health plan or insurance company must notify covered employees of the availability of the notice and how it can be obtained at least once per three year period.

(§164.520(c)(1) - Provision of Notice)

If a covered entity maintains a web site that provides information about the covered entity's customer services or benefits, it must prominently post its Privacy Notice on the web site and make it available electronically through the web site.

(§164.520(c)(3) - Provision of Notice)

A Privacy Notice is required to be written in plain language and contain, at a minimum, the specific provisions outlined in the regulation. Attachment 2 - Privacy Notice contains a listing of the required provisions.

(§164.520(b) - Content of Notice)

DISCLOSURE OF PROTECTED HEALTH INFORMATION TO THE PLAN SPONSOR

In order for the employer that sponsors a group health plan to receive protected health information from the self funded plan, insurance company or HMO, the self funded plan, insurance company or HMO must receive verification from the employer that the plan documents have been amended to restrict uses and disclosures by the employer as required by the regulation. In the case of a fully insured plan, this requirement does not apply to the provision of summary health information for the purposes of obtaining premium quotes, or modifying or terminating the plan or to information regarding the enrollment and termination of individuals under the plan.

(§164.504(f)(1) - Requirements for Group Health Plans)

Disclosures to the employer must be limited to disclosures necessary to carry out plan administration functions that the employer performs and may not be made unless a statement is included in the appropriate Privacy Notice regarding the employer's receipt of such information. A group health plan is prohibited from disclosing protected health information to the employer for purposes of employment related decisions or in connection with any other benefit plan.

(§164.504(f)(3) - Uses and Disclosures)

The regulations require that the plan documents of an employer that receives protected health information include specific provisions as outlined in the regulation. Attachment 3 – Plan Document Amendment contains a listing of the required provisions. *(§164.504(f)(2) - Requirements for Plan Documents)*

CONSENTS

Covered entities are not required to obtain a consent prior to using or disclosing protected health information for the purposes of treatment, payment or health care operations, but is allowed to voluntarily seek consent if they choose to. A covered entity is allowed to make disclosures to another covered entity or health care provider for payment purposes of that entity. (§164.506 - *Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations*)

AUTHORIZATIONS

General Rule

An authorization is required for any use or disclosure of protected health information other than:

- Disclosures to the individual that is the subject of the information;
- Disclosures for purposes of treatment, payment and health care operations;
- Disclosures required by law;
- Disclosures related to public health activities;
- Disclosures to a health oversight agency in relation to oversight activities of that agency;
- Disclosures required as part of a judicial or administrative hearing;
- Disclosures for law enforcement purposes.

(§164.508(a)(1) - *General Rule*)

An authorization can be revoked at any time by the individual, provided such revocation is in writing.

(§164.508(b)(5) - *Revocation of Authorizations*)

Authorizations are required to be maintained on file for a period of six years.

(§164.508(b)(6) - *Documentation*)

Marketing

A covered entity cannot use or disclose protected health information for marketing purposes without a signed authorization, except in the case of marketing communications that:

- Are made face to face with the individual; or
- Concern products or services of nominal value.

If the covered entity will receive direct or indirect remuneration for making the marketing communication, the authorization must state the covered entity is receiving payment.

(§164.508(3) - *Authorization Required Marketing*)

Provided that there is not direct or indirect payment from a third party, marketing does not include communications:

- To describe a health related service or product provided or included in a plan of benefits;
- Made in the course of managing the treatment of that individual; or
- For the purpose of recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

(§164.501 - *Definitions*)

Psychotherapy Notes

Except for the following limited exceptions, any use or disclosure of psychotherapy notes requires a signed authorization:

- Use in providing treatment by the health care provider that made the notes;
- Use or disclosure in training programs for students or practitioners in mental health to improve their counseling skills;
- Use or disclosure to defend against a legal action or other proceeding brought by the individual;
- As required by the Secretary of Health and Human Services to determine a covered entity's compliance with the regulation;
- As required by law;
- For health oversight activities with respect to the originator of the notes;
- For reasons of public safety.

(§164.508(a)(2) - Authorization Required Psychotherapy Notes)

Prohibition on Conditioning of Authorizations

A covered entity can never condition the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the individual signing an authorization in relation to psychotherapy notes. And can only condition the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the individual signing an authorization for other than psychotherapy notes in the following circumstances:

- A health plan can condition enrollment in the plan or eligibility for benefits, if the authorization is sought prior to enrollment in the plan and is for use in eligibility determinations, underwriting or risk rating only;

(§164.508(b)(4) - Prohibition on Conditioning Authorizations)

Requirements for a Valid Authorization

An authorization for use or disclosure of protected health information cannot be combined with any other document or authorization, except for another authorization for the use or disclosure of protected health information, other than for psychotherapy notes. If an authorization conditions treatment, payment, enrollment in a health plan or eligibility for benefits on signing the authorization, it must be presented separately and cannot be combined with other authorizations. Authorizations for the use and disclosure of psychotherapy notes can only be combined with other authorizations for psychotherapy notes. *(§164.508(b)(3) - Compound Authorizations)*

An authorization must be written in plain language and contain, at a minimum, the specific provisions outlined in the regulation. Attachment 4 - Authorization contains a listing of the required provisions.

USES AND DISCLOSURES REQUIRING OPPORTUNITY TO AGREE OR OBJECT

In the following circumstances a covered entity can use or disclose protected health information, provided that it informs the individual prior to the use or disclosure and allows the individual the opportunity to agree, prohibit or restrict the use or disclosure. If the individual does not agree to the use or disclosure or restricts it, the covered entity must abide by that decision.

- Disclosure to a family member, other relative or any other person identified by the individual, of protected health information directly relevant to the person's involvement with the individual's health care or payment for health care;
- Disclosure of protected health information to notify or assist in notification, including identifying or locating a family member or personal representative, of the individual's location, general condition or death.

(§164.510(b) - Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes)

INDIVIDUAL'S RIGHT TO REQUEST RESTRICTIONS ON USES AND DISCLOSURES

A covered entity is required to allow an individual to request that the covered entity restrict its uses and disclosures in relation to treatment, payment and health care operations, and in relation to uses and disclosures to persons involved in the individual's care or for notification purposes. A covered entity is not required to agree to a requested restriction.

If a covered entity does agree to a requested restriction, it is prohibited from using or disclosing protected health information in violation of the restriction unless the individual who is the subject of the information is in need of emergency treatment and the restricted information is necessary to provide that treatment. A covered entity can terminate its agreement to a restriction upon the request of the individual, with individual's agreement, or for future protected health information only by informing the individual that it is terminating the agreement.

(§164.522 - Rights to Request Privacy Protection for Protected Health Information)

Confidential Communications

A health plan must accommodate an individual's reasonable request to receive communications of protected health information by an alternative means or at an alternative location, if the individual clearly states that disclosure could endanger them. A health plan can require that the request be made in writing and include a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

(§164.522(b) - Confidential Communications Requirements)

INDIVIDUAL'S RIGHT TO ACCESS PROTECTED HEALTH INFORMATION

A covered entity must provide an individual access to inspect and obtain a copy of protected health information about the individual that is held in a designated record set, for as long as the information is maintained in the designated record set. A covered entity may only deny access to the individual under the following circumstances:

- Without a right to review of the denial, if:
 - The information is psychotherapy notes
 - The information has been compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding
 - The information is subject to the Privacy Act, 5 U.S.C. §552a, and the denial meets the requirements of that law
 - The information was received from a source, other than a health care provider, that requested confidentiality and the access would be reasonably likely to reveal that source;
- With a right to review of the denial by a licensed health care professional designated by the covered entity and not involved in the original denial, if:
 - A licensed health care professional has determined that access is likely to endanger the life or physical safety of the individual or another person
 - A licensed health care professional has determined that access is likely to cause substantial harm to another person referenced in the information
 - The request is made by a personal representative and a license health care professional has determined that access is likely to cause substantial harm to the individual that is the subject of the information or another person.

(§164.524(a) - Access to Protected Health Information)

A covered entity must respond to a request for access to protected health information by either informing the individual of its acceptance of the request or providing the individual with a written denial within 30 days of receipt of the request. If requested information is not maintained on-site, the covered entity may take up to 60 days from receipt of the request to respond. If the covered entity is unable to respond within the 30 or 60 day time frame as applicable, it may take a 30 day extension by informing the individual of the reason for the delay and a date by which it will complete action on the request. *(§164.524(b) - Request for Access and Timely Action)*

A covered entity must document and retain the documentation for six years the designated record sets that are subject to access by individuals and the titles or offices of the persons responsible for receiving and processing requests for access by individuals. (*§164.524(e) - Documentation*)

Providing Requested Access

If the covered entity agrees to the request for access to protected health information, it must provide the individual with access to the information in the form or format requested if it is readily producible in that form or format. If it is not available in the request form or format, it must be provided in a readable hard copy form or another form or format as agreed to with the individual.

If the individual agrees in advance to receiving a summary of the protected health information and to any fee that may be charged for the summary, a covered entity may provide the individual with a summary in lieu of access to the actual protected health information.

If the individual request a copy of the information, the covered entity may charge a reasonable, cost-based fee for copying and postage.

(*§164.524(c) - Provision of Access*)

Denial of Access

If the covered entity denies access, in whole or in part, it must provide a written denial to the individual that is in plain language and includes the following:

- The basis for the denial;
- A statement of the right to review of the denial, if applicable;
- A description of how the individual may complain to the covered entity or the Secretary of Health and Human Services.

If the denial is because the covered entity does not maintain the protected health information requested and the covered entity knows where the information is maintained, it is required to inform the individual where to direct the request.

(*§164.524(d) - Denial of Access*)

INDIVIDUAL'S RIGHT TO AMEND PROTECTED HEALTH INFORMATION

A covered entity must amend, at the request of the individual, protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in a designated record set. A covered entity may only deny a request for amendment, if it determines that the protected health information or record:

- Was not created by the covered entity, unless the individual shows that the originator of the information is no longer available to act on the request;
- Is not part of a designated record set;
- Is not required to be made available for inspection by the individual; or
- Is accurate and complete.

(*§164.526(a) - Right to Amend*)

A covered entity may require that a request for amendment be in writing and provide a reason for the requested amendment. A covered entity must respond to a request for amendment of protected health information by either informing the individual of its acceptance of the request or providing the individual with a written denial within 60 days of receipt of the request. If the covered entity is unable to respond within the 30 or 60 day time frame as applicable, it may take a 30 day extension by informing the individual of the reason for the delay and a date by which it will complete action on the request. (*§164.526(b) - Requests for Amendment and Timely Action*)

A covered entity that is informed by another covered entity of an amendment to the individual's protected health information must amend the information in their designated records sets.

(§164.526(e) - Actions on Notices of Amendment)

A covered entity must document the titles or offices of the persons responsible for receiving and processing requests for amendment and maintain that documentation for a period of six years.

(§164.526(f) - Documentation)

Agreement to Amend

If a covered entity agrees to amend the protected health information it must, at minimum, identify the records that are affected by the amendment and append or otherwise link those records to the amendment. The covered entity must then make reasonable efforts to provide the amendment to those persons identified by the individual as having received the protected health information and needing the amendment, and any persons, including business associates, that the covered entity knows received the protected health information that was amended and may rely on it to the detriment of the individual. *(§164.526(c) - Accepting the Amendment)*

Denial of Amendment

If the covered entity denies the request for amendment, in whole or in part, it must provide a written denial to the individual that is in plain language and includes the following:

- The basis for the denial;
- A statement of the right to submit a statement disagreeing with the denial and how to file such statement;
- A statement that if a statement of disagreement is not filed, the individual may request that the request for amendment and the denial be included with any future disclosures of the information;
- A description of how the individual may complain to the covered entity or the Secretary of Health and Human Services.

The covered entity must permit the individual to submit a written statement of disagreement with any denial of a request to amend protected health information and the basis for the disagreement. The covered entity may reasonably limit the length of such statement. If a statement of disagreement is filed, the covered entity may include a written rebuttal to it with the information provided it gives the individual a copy of the rebuttal.

The covered entity is required to identify the records affected by the denied request for amendment and append or otherwise link the records to the request for amendment, the denial, and if applicable, any statement of disagreement and rebuttal. Any future disclosures of the information must include this appended or linked information or at the option of the covered entity an accurate summary of the appended or linked information. If disclosure is by standard electronic transaction and the transaction does not allow for the inclusion of such information, the covered entity may transmit the appended or linked information separately.

(§164.526(d) - Denying the Amendment)

INDIVIDUAL'S RIGHT TO AN ACCOUNTING OF DISCLOSURES

A covered entity is not required to provide an accounting of the following types of disclosures, as allowed under the regulation:

- Disclosures to carry out treatment, payment and health care operations;
- Disclosures under a signed authorization from the individual;
- Disclosures made to the individual that is the subject of the information;
- Disclosures that are incidental to a use or disclosure otherwise permitted under the regulation;
- Disclosures that are made as part of a limited data set;
- Disclosures made to persons involved in the individual's care or for notification purposes;

- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials;
- Disclosures that occurred prior to the covered entity's compliance date with the regulation.

If the covered entity has made disclosures of protected health information for reasons other than those stated above, it must, at the individual's request, provide an accounting of those disclosures for up to six years prior to the date of the request for accounting.

(§164.528(a) - Right to an Accounting of Disclosures of Protected Health Information)

If an accounting of disclosures is required, the covered entity must provide a written accounting that includes the following elements for each disclosure within 60 days of the receipt of the request for accounting:

- The date of the disclosure;
- The name of the entity or person who received the protected health information and, if known, the address;
- A brief description of the protected health information disclosed; and
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

If multiple disclosures for the same purpose were made to a single entity, accounting of the disclosures may be made by accounting for the first disclosure as outlined above and including a statement of the frequency or number of disclosures to that entity and the last date within the accounting period of a disclosure to that entity.

(§164.528(b) - Content of the Accounting)

REQUIREMENTS FOR COVERED ENTITIES

Except for requirements relating to the prohibition of retaliatory acts and the prohibition of requiring waiver of rights under the regulation, a group health plan that is fully insured and receives only summary health information and information on enrollment and termination is not subject to the requirements for covered entities.

(§164.530(k) - Group Health Plans)

Covered entities, including self funded group health plans, are required to:

- Designate a Privacy Officer who is responsible for developing policies and procedures necessary for compliance with the regulation;
- Designate a contact person or office that is responsible for receiving complaints and providing information regarding the Notice of Privacy Practices;
- Provide training regarding privacy policies and procedures to all employees, if necessary or appropriate for the employee to be able to do their job. Such training must be provided by the compliance date of the covered entity for existing employees, to each new employee within a reasonable period of time of their hire, and as necessary due to changes in policy or procedure;
- Put in place reasonable and appropriate administrative, technical and physical safeguards to prevent the, intentional or unintentional, use or disclosure of protected health information in violation of the regulation, and to limit incidental uses and disclosures in relation to those that are permitted under the regulation;
- Provide a process for individuals to file complaints regarding the covered entity's privacy policies and procedures or its compliance with the regulation;
- Put in place and apply appropriate sanctions for employees who fail to comply with privacy policies and procedures of the covered entity or who violate the regulation;
- Mitigate, to the extent practical, any harmful effect that is known to the covered entity and resulted from the use or disclosure of protected health information by the covered entity or its business associates in violation of the covered entity's privacy policies and procedures or in violation of the regulation;
- Not discriminate against or take retaliatory action against an individual who exercises their rights under the regulation;

- Not require an individual to waive their rights under the regulation as a condition of receiving treatment, payment, enrollment in a health plan or eligibility for benefits;
 - Implement policies and procedures that are reasonably designed to comply with the requirements of the regulation, taking into account the size and activities of the covered entity.
- (§164.530 - Administrative Requirements)*

Documentation Requirements

A covered entity must maintain, in written or electronic form, the following information for a period of six years from the date of the information's creation or if later its last revision:

- Documentation of the personnel designations of a Privacy Officer and person or office to receive complaints and handle inquiries on Privacy Notices;
- Documentation of the provision of privacy training to employees;
- All complaints regarding privacy received by the covered entity and their disposition;
- All sanctions applied against employees for violating privacy policies and procedures;
- Privacy policies and procedures of the covered entity;
- Any communication that is required by the regulation to be in writing (e.g. consents, authorizations);
- Any activity, designation or action that is required to be documented by the regulation (e.g. Privacy Notices, agreement restrictions of use, designation of personnel to handle request for access and amendment).

(§164.530(j) - Documentation)

PRE-EMPTION OF STATE LAWS

In general the Privacy Regulations pre-empt State laws regarding privacy to the extent that the State law is not more stringent than the Federal Regulations.

(§160.203 - General Rule and Exceptions)

PENALTIES

In addition to the standard penalties under ERISA, the HIPAA statute establishes the following maximum penalties in relation to privacy violations: \$50,000 in fines and/or one year imprisonment for knowingly obtaining or disclosing protected health information or unique health identifiers; \$100,000 in fines and/or five years imprisonment if the offense is committed under false pretenses; and \$250,000 in fines and/or 10 years imprisonment if the offense is committed with intent sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.

(HIPAA Title II Subtitle F §262 - Wrongful Disclosure of Individually Identifiable Health Information)

ATTACHMENT 1 - BUSINESS ASSOCIATE AGREEMENT

A Business Associate Agreement is required to contain the following elements at a minimum:

- The permitted and required uses and disclosures of information by the business associate. It cannot authorize a use or disclosure that would violate the obligations of the covered entity under this regulation;
- Requirements that the business associate will:
 - Not use or further disclose the information other than as allowed in the contract
 - Use appropriate safeguards to prevent unauthorized use or disclosure of the information
 - Report to the covered entity any use or disclosure of the information not allowed in the contract
 - Ensure that any agents, including a subcontractor, to whom it provides protected health information agrees to the same restrictions and conditions that apply to the business associate
 - Make protected health information available for inspection by the individual that is the subject of the information
 - Make protected health information available for amendment and incorporate any amendments to the information
 - Make available the information required to provide an accounting of disclosures
 - Make its internal practices, books, and records relating to the use and disclosure of protected health information available to the Secretary for purposes of determining the covered entity's compliance
 - At termination of the contract return or destroy all protected health information or, if that is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those reasons that make its return or destruction infeasible;
- A provision authorizing termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

ATTACHMENT 2 - PRIVACY NOTICE

A Privacy Notice is required to contain the following elements at a minimum:

- The following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”;
- A description, including at least one example, of the types of uses and disclosures that may be made in relation to treatment, payment, and health care operations;
- A description of each of the other purposes for which protected health information may be used or disclosed without the individual’s written consent or authorization;
- A statement that other uses and disclosures will be made only with the individual’s written authorization and that the individual may revoke such authorization;
- If applicable, a separate statement relating to each of the following activities: contact to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual; contact to raise funds for the covered entity; or that a group health plan, or a health insurance issuer or HMO may disclose protected health information to the sponsor of the plan;
- A statement of the individual’s rights with respect to protected health information and a brief description of how the individual may exercise these rights including the right to request restrictions on certain uses and disclosures, the right to receive confidential communications, the right to inspect and copy protected health information, the right to amend protected health information, the right to receive an accounting of disclosures of protected health information, and the right of an individual to obtain a paper copy of the notice from the covered entity upon request;
- A statement that the covered entity is required by law to maintain the privacy of protected health information and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information;
- A statement that the covered entity is required to abide by the terms of the notice currently in effect;
- If changes in the Privacy Notice are to apply to information existing at the time of the change, a statement that the covered entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.
- A statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.
- The name, or title, and telephone number of a person or office to contact for further information;
- The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

ATTACHMENT 3 – PLAN DOCUMENT AMENDMENT

The plan documents of an employer that receives protected health information are required to contain the following elements:

- The permitted and required uses and disclosures of such information by the plan sponsor;
- Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification that the plan documents have been amended to indicate that the plan sponsor agrees to:
 - Not use or further disclose the information other than as permitted by the plan documents or as required by law
 - Ensure that any agents, including a subcontractor, agree to the same restrictions that apply to the plan sponsor
 - Not use or disclose the information for employment-related actions and decisions or in connection with any other employee benefit plan of the plan sponsor
 - Report to the group health plan any use or disclosure of the information that is inconsistent with the terms of the plan document
 - Make protected health information available for inspection by the individual that is the subject of the information
 - Make protected health information available for amendment and incorporate any amendments to the information
 - Make available the information required to provide an accounting of disclosures
 - Make its internal practices, books, and records relating to the use and disclosure of protected health information available to the Secretary for purposes of determining the group health plan's compliance
 - Destroy all protected health information when it is no longer necessary for the purposes for which it was provided or, if that is not feasible, limit further uses and disclosures to those reasons that make its return or destruction infeasible
 - Ensure that the adequate separation between the group health plan and plan sponsor is established by describing the employees, classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information and restricting their access and use to the plan administration functions that the plan sponsor performs for the group health plan
 - Provide an effective mechanism for resolving any issues of noncompliance by persons at the plan sponsor.

ATTACHMENT 4 – AUTHORIZATION

An authorization is required to contain the following elements at a minimum:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful way;
- The name or other specific identification of the person or entity making the request;
- The name or other specific identification of the person or entity, to whom the covered entity may make the requested use or disclosure;
- A description of each purpose of the requested use or disclosure;
- An expiration date or an expiration event;
- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual;
- A statement of the individual's right to revoke the authorization in writing and either the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization, or reference to the Covered Entity's Privacy Notice if that information is included in that notice;
- A statement indicating that the plan may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization, or in the case of a pre-enrollment authorization sought by the plan as allowed under the regulation, a statement indicating the consequences of refusing to sign the authorization;
- A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;

If the authorization is for a covered entity's own use and disclosure of protected health information, the covered entity is required to provide a copy of the signed authorization to the individual.