

Privacy Assessment Instructions

The tool is set up in a matrix fashion, following the final regulation. The section of the regulation that the question refers to is listed and named. The “Rule Comments” column gives a brief statement of what is required / allowed by the regulation. The wording of these, for the most part, comes directly from the published rule.

Complete the questionnaire by writing your response to the question in the “Response” column. If you need more space for any questions attach your answers on a separate paper referenced by the question number (Q#). If an issue or topic is not relevant to you, write “N/A” in the response column. For example, if you do not do research or produce psychotherapy notes. Include in your response reference to any current policy and procedure that addresses that issue.

In the process of completing the questionnaire you will be identifying uses and disclosures of protected health information and to whom the information is disclosed. Record these on the attached “Use and Disclosure List.” Include on this list those uses and disclosures that may not be identified in the course of filling out the questionnaire. For example, also list any additional business partners you share information with that are not identified in the course of the questionnaire. For example, those you share information with for payment, treatment, and normal business operations.

After the questionnaire and list are completed for all areas of your company, identify gaps and begin developing a plan to address them. For example:

- Review all referenced policies and procedures and update or develop as needed.
- Review all business partner agreements/contracts for compliance.
- Identify minimum necessary requirements for information subject to them
- Implement authorization processes and model form.
- Identify processes for de-identifying information
- Once all policies and procedures are updated/developed, develop the Notice of Privacy Practices.

Attachment 1: Definitions (Revised per Final Rule)

Protected Health Information (PHI): Protected health information is defined as individually identifiable health information that transmitted by electronic media, maintained in any medium as described in the definition of electronic media at 162.103 of this subchapter, and transmitted or maintained in any other form or medium. Individually Identifiable Health Information is defined as health information including demographic information, collected from an individual and 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 the individual; the provision of health care to an individual, and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Psychotherapy Notes are defined as notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Such term would not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, or a brief summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

Attachment 2: Consent for Treatment, Payment, or Health Care Operations

The following are general requirements and implementation specifications for obtaining consent for uses or disclosures of protected health information for treatment, payment or health care operations.

- Failure to obtain a consent must be documented. The documentation must contain information about the attempt to obtain consent and the reason why consent was not obtained.
- A consent obtained by one covered entity is not effective to permit another covered entity to use or disclose protected health information.
- A provider may condition treatment on the provision of obtaining a consent and a health plan may condition enrollment on the provision of obtaining a consent.
- The consent may not be combined in a single document with the Notice of Privacy Practices.
- The consent may be combined with other written legal permission from the individual if the consent for treatment, payment, or health care operations is visually and organizationally separate from other written legal permission and is separately signed and dated by the individual.
- A consent may be combined with a research authorization that meets the research authorization requirements of the regulation (164.508(f)).

- An individual may revoke, in writing, a consent at anytime except to the extent that the covered entity has already taken action on the existing consent.
- Signed consents must be documented and retained in original or electronic copy for six years from the date of creation or the date when it was last in effect, whichever is later.
- A consent must meet the following content requirements:
 - Be in plain language;
 - Inform the individual that PHI may be used and disclosed to carry out treatment, payment, or health care operations;
 - Refer the individual to the Notice of Privacy Practices for a more complete description of such uses and disclosures;
 - State that the individual has the right to review the Notice of Privacy Practices prior to signing the consent;
 - If the covered entity has reserved the right to change its privacy practices, state that the terms of the notice may change and describe how the individual may obtain a revised notice;
 - State that the individual has the right to request a restriction on how his/her PHI is used or disclosed to carry out payment, treatment, and health care operations (The covered entity is not required to agree to restrictions, but if it does, it must follow them);
 - State that the individual has the right to revoke the consent in writing, except to the extent that action has already been taken on the initial consent;
 - Be signed by the individual and dated.
- The consent is considered defective, and therefore not valid, if it lacks any of required elements or has been revoked.
- If there is a conflict between an obtained consent and any other authorization or written legal permission for disclosure of PHI for payment, treatment, or health care operations, use and disclosure must follow the more restrictive document.
- Attempts may be made to resolve the conflict by obtaining a new consent, or communicating (orally or in writing) with the individual to determine the individual's preference for resolving the conflict. The individual's preference must be documented and the covered entity must follow this preference.
- If a covered entity participates in an organized health care arrangement, a joint consent may be used. A joint consent must
 - Include the name or other specific identification of the covered entities to which the consent applies
 - Meet all the other requirements of a valid consent, except required statements may be altered to reflect that the consent covers more than one covered entity.
- If an individual revokes a joint consent, the entity receiving the revocation must inform all other entities covered by the consent of the revocation as soon as practicable.

Attachment 3: Exceptions to Authorization for Use or Disclosure of Psychotherapy Notes.

If a valid consent is obtained for treatment, payment, and health care operations, an additional authorization for use or disclosure of psychotherapy notes is not required under the following situations:

- Use by the originator of the notes for treatment;
- Use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
- Use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual;
- Use or disclosure required by the Secretary (of DHH) to investigate or determine the covered entity's compliance with this regulation;
- Use or disclosure is required by law and is limited to the relevant requirements of such law;
- Disclosure to a health oversight agency for activities with respect to the oversight of the originator of the psychotherapy notes;
- Disclosure to coroners and medical examiners for the purpose of identifying a deceased individual, determining a cause of death, or other duties as authorized by law;
- If a belief (in good faith of the covered entity) that disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

Attachment 4: Authorizations

The regulation spells out the requirements for valid authorizations as well as use of compound authorizations and a prohibition on conditioning of authorizations. A valid authorization is a document that contains the core elements and, as applicable, the elements required in authorizations requested by a covered entity for its own use and disclosures; authorizations requested by a covered entity for disclosure by others; and authorizations for uses and disclosures of PHI created for research that includes treatment of the individual.

The core elements of a valid authorization are:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

- A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
- A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by this rule;
- 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;
- The authorization must also be written in plain language.

Authorizations requested by a covered entity for its own uses and disclosures, in addition to containing the core elements listed above, must include the following elements:

- A statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure, if the requested use or disclosure is prohibited by the regulation (See Attachment 6 for the prohibitions for conditioning);
- A description of each purpose of the requested use or disclosure;
- A statement that the individual may:
 - inspect or copy the PHI to be used or disclosed;
 - refuse to sign the authorization; and
 - if the use or disclosure will result in direct or indirect remuneration to the covered entity from a third party, a statement of such remuneration;
- A copy of the signed authorization must also be given to the individual.

Authorizations requested by a covered entity for disclosure by other covered entities, in addition to containing the core elements listed above, must include the following elements:

- A description of each purpose of the requested disclosure;
- Except for an authorization upon which payment may be conditioned, a statement that the covered entity will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure (A health plan may condition payment of a claim for specified benefits on provision of an authorization if the disclosure is necessary to determine payment of the claim and the authorization is not for a use or disclosure of psychotherapy notes.);
- A statement that the individual may refuse to sign the authorization.
- A copy of the signed authorization must also be given to the individual.

Authorizations for uses and disclosures of PHI created for research that includes treatment of the individual must be obtained, except for research purposes as permitted by the regulation (See Attachment 14 for a description of these exceptions). Such authorizations must contain all the core elements listed above, the additional elements required for authorizations requested by a covered entity for its own uses and disclosures, as well as the following:

- A description of the extent to which such protected health information will be used or disclosed to carry out treatment, payment, or health care operations;

- A description of any PHI that will not be used or disclosed for purposes permitted in accordance with uses and disclosures requiring an opportunity for the individual to agree or object and uses and disclosures for which consent, and authorization, or opportunity to agree or object is not required, provided that covered entity may not include a limitation affecting its right to make a use or disclosure that is required by law or necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
- If the covered entity has obtained or intends to obtain a consent for treatment, payment, or health care operations, or has provided or intends to provide a Notice of Privacy Practices, the authorization must refer to that consent or notice, as applicable, and state that the statements made are binding.
- These types of research authorizations may be in the same document as a consent to participate in the research; a consent to use or disclose PHI to carry out treatment, payment, or health care operations; or a notice of privacy practices.

An authorization with any of the following defects is considered not valid and may not be used or acted upon.

- The expiration date has passed or the expiration event is known (by the covered entity) to have occurred;
- The authorization has not been filled out completely, with respect to the required elements listed above;
- The authorization is known by the covered entity to have been revoked;
- The authorization lacks any of the required elements listed above;
- The authorization violates the conditions for allowable use of a compound or combined authorization (see Attachment 5);
- Any material information in the authorization is known by the covered entity to be false.

Attachment 5: Compound Authorizations

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

- An authorization for the use or disclosure of PHI created for research that includes treatment of the individual may be combined with other authorizations as indicated above (See Attachment 4);
- An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;
- An authorization (other than that for psychotherapy notes) may be combined with any other authorization allowed for under “Uses and disclosures for which an authorization is required” (164.508), except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the authorizations.

Attachment 6: Prohibition on Conditioning of Authorizations

A covered entity may not condition the provision of treatment, payment, enrollment in the health plan, or eligibility of benefits on the provision of an authorization except under the following circumstances:

- A covered health care provider may condition the provision of research related treatment on a provision of an authorization that meets the requirements listed in Attachment 4;
- A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan if:
 - The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and
 - The authorization is not for a use or disclosure of psychotherapy notes.
- A health plan may condition payment of a claim for specified benefits on provision of an authorization "requested by a covered entity for disclosures by others" if:
 - The disclosure is necessary to determine payment of the claim; and
 - The authorization is not for a use or disclosure of psychotherapy notes.
- A covered entity may condition 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 the PHI to the third party.

Attachment 7: Use and Disclosure for a Facility Directory – Emergency Circumstances

If the opportunity to object to uses or disclosures of PHI in a facility directory cannot be provided because of the individual's incapacity or an emergency treatment circumstance, some or all of the allowable PHI may be used in a facility directory if such use is:

- Consistent with a prior expressed preference of the individual, if any, that is known by the covered health care provider, and
- In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

Attachment 8: Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes.

The disclosure requirements that must be met to release PHI to a family member, other relative, etc. to the extent that that person is involved in the individual's care or payment related to care, or for notification purposes are:

If the individual is present for, or otherwise available prior to the use or disclosure and has the capacity to make health care decisions, the covered entity must:

- Obtain the individual's agreement;

- Provide the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
- Reasonably infer from the circumstances, based on professional judgment, that the individual does not object to the disclosure.

If the individual is not present, or the opportunity to object cannot practicably be provided due to the individual's incapacity or emergency situation, the covered entity may:

- Exercise professional judgment to determine whether the disclosure is in the best interest of the individual; and
- Only disclose the PHI that is directly relevant to the person's involvement with the individual's care.

Furthermore, a covered entity may disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses and disclosures noted above (e.g., disclosures for involvement in the individual's care and disclosures for notification). The covered entity must meet the disclosure requirements listed above to the extent that, under professional judgment, the requirements do not interfere with the ability to respond to the emergency circumstances.

Attachment 9: Restrictions for Disclosure to an Employer

Disclosure of PHI to an employer is allowed, without written consent or authorization, or opportunity to agree or object, if the covered entity is a covered health care provider who is a member of the workforce of the employer or provides health care at the request of the provider. The disclosures are limited to conducting an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work related illness or injury. Further restrictions require:

- Limiting the PHI disclosed to findings concerning a work related illness or injury, or a workplace related medical surveillance;
- The employer to need such information in order to comply with its obligations under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose;
- The covered health care provider to provide written notice to the individual that PHI relating to the surveillance or work related illnesses and injuries is disclosed to the employer. This may be done by:
 - Giving a copy of the notice to the individual at the time the health care is provided; or
 - If health care is provided on the work site of the employer, by posting the notice in a prominent location where the care is provided.

Attachment 10: Restrictions Related to Disclosures about Victims of Abuse, Neglect, or Domestic Violence.

A covered entity may disclose PHI about an individual about whom the entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive such reports with the following restrictions: (Reports of child abuse or neglect given to the appropriately authorized organizations are exempted from these restrictions.)

- Disclosure is allowed to the extent it is required by law, complies with the law, and is limited to the relevant requirements of the law;
- The individual agrees with the disclosure; or
- The disclosure is to the extent expressly authorized by statute or regulation; and
- The covered entity, in professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
- The individual is unable to agree due to incapacity, the authorized recipient of the PHI represents that the information will not be used against the individual, and an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A covered entity who makes such a disclosure must inform the individual that such a report has been or will be made, except if:

- The covered entity, in professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The covered entity would be informing a personal representative, and reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and informing such person would not be in the best interest of the individual, in the entity's professional judgment.

Attachment 11: Conditions under which Information may be Released for Judicial and Administrative Proceedings.

Disclosure of PHI may be made in the course of judicial and administrative proceedings under the following conditions:

- In response to a court order or administrative tribunal, provided only the PHI expressly authorized is disclosed; or
- In response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order or administrative tribunal if:
 - The covered entity receives a written statement and accompanying documentation showing that the requestors of the PHI showed a good faith effort to provide written notice to the individual;
 - The notice contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
 - The time for the objections has elapsed and no objections were filed, or all filed objections have been resolved and the disclosure is consistent with the resolution.
- The covered entity receives written statement and accompanying documentation that:

- The parties to the dispute giving rise to the request for the information have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or
- The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal;
- A qualified protective order is defined as an order of a court or an administrative tribunal or stipulation by the parties in the litigation or administrative proceeding that prohibits the parties from using or disclosing the PHI for any other purpose other than for which the information was requested, and requires the return to the covered entity or destruction of the PHI at the end of the litigation or proceeding.
- However, if the covered entity itself makes reasonable efforts to provide notice to the individual or seeks a qualified protective order, it may disclose PHI in response to lawful process without receiving a written statement and documentation of the requesting persons attempt to notify the individual of the disclosure.

Attachment 12: Conditions for Disclosures for Law Enforcement

The regulation authorizes disclosure of certain PHI pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:

- As required by law, including laws that require the reporting of certain types of wounds or other physical injuries, (except for laws related to disclosure about reports of child abuse or neglect, and except for laws related to disclosure about victims of abuse, neglect, or domestic violence); or
- In compliance with and as limited by the relevant requirements of
 - a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
 - a grand jury subpoena; or
 - an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
 - the information sought is relevant and material to a legitimate law enforcement inquiry;
 - the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
 - de-identified information could not reasonably be used.

Attachment 13: Conditions for Disclosure of Information about Victims of a Crime

A covered entity may disclose PHI about a victim of a crime without written consent or authorization, or opportunity to agree or object under certain conditions.

- The covered entity may disclose information required by law as permitted for identification and location purposes;
- The covered entity may disclose information if it falls under the requirements for uses and disclosures permitted for public health activities;

- The covered entity may disclose information if it falls under the requirements for disclosures about victims of abuse, neglect, or domestic violence;
- The entity may disclose information about a crime victim if:
 - The individual agrees to the disclosure,
 - The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and
 - The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

Attachment 14: Conditions for Use and Disclosure of Information for Research

A covered entity may use or disclose PHI for research, regardless of the source of funding, provided that:

- Documentation is obtained from a qualified Institutional Review Board or privacy board that an alteration or waiver, in whole or part, of the individual authorization form (as required in the section of “uses and disclosures for which an authorization is required”) has been approved. (See below for the criteria of a qualified IRB and qualified privacy board and the required components of the documentation.)
- The researcher has provided that:
 - Use and disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes to prepare for the research;
 - No PHI is to be removed from the covered entity by the researcher in the course of the review; and
 - The PHI for which access is sought is necessary for the research purposes.
- If decedent’s information is to be used, the researcher must provide:
 - Representation that the use or disclosure sought is solely for research on the PHI of decedents;
 - Documentation (at the request of the covered entity) of the death of such individuals; and
 - Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

An Institutional Review Board must be established in accordance with any of the regulations listed below:

7 CFR 1c.107	10 CFR 745.107	14 CFR 1230.107	15 CFR 27.107
16 CFR 1028.107	21 CFR 56.107	22 CFR 225.107	24 CFR 60.107
28 CFR 46.107	32 CFR 219.107	34 CFR 97.107	38 CFR 16.107
40 CFR 26.107	45 CFR 46.107	45 CFR 690.107	49 CFR 11.107

A privacy board must meet the following criteria:

- Have members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual’s privacy rights and related interests.

- Includes at least one member who is not affiliated with the covered entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entities.
- Does not have any member participating in a review of any project in which the member has a conflict of interest.

Documentation of waiver approval. For use and disclosure to be permitted based on the documentation of approval of an alteration or waiver, the documentation must include:

- A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;
- A statement that the IRB or privacy board had determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
 - The use or disclosure of PHI involves no more than minimal risk to the individuals;
 - The alteration or waiver will not adversely affect the privacy rights and welfare of the individuals;
 - The research could not practicably be conducted without the alteration or waiver;
 - The research could not practicably be conducted without access to and use of the PHI;
 - The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and the importance of the knowledge that may reasonably be expected to result from the research;
 - There is an adequate plan to protect the identifiers from improper use and disclosure;
 - There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law;
 - There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as permitted by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this regulation.
- A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board (meeting the condition stated above that the research could not practicably be conducted without the alteration or waiver).
- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as follows:

- An IRB must follow the requirements of the Common Rule, including the normal review procedures found in

7 CFR 1c.108(b)	10 CFR 745.108(b)	14 CFR 1230.108(b)	15 CFR 27.108(b)
16 CFR 1028.108(b)	21 CFR 56.108(b)	22 CFR 225.108(b)	24 CFR 60.108(b)
28 CFR 46.108(b)	32 CFR 219.108(b)	34 CFR 97.108(b)	38 CFR 16.108(b)
40 CFR 26.108(b)	45 CFR 46.108(b)	45 CFR 690.108(b)	49 CFR 11.108(b)

or the expedited review procedures found in

7 CFR 1c.110	10 CFR 745.110	14 CFR 1230.1101	15 CFR 27.110
--------------	----------------	------------------	---------------

16 CFR 1028.110	21 CFR 56.110	22 CFR 225.110	24 CFR 60.110
28 CFR 46.110	32 CFR 219.110	34 CFR 97.110	38 CFR 16.110
40 CFR 26.110	45 CFR 46.110	45 CFR 690.110	49 CFR 11.110

- A privacy board must review the proposed research at convened meetings at which a majority of members is present, including one member who satisfies the criteria on non-affiliation or conflict of interest noted above, and the alteration or waiver of authorization must be approved by the majority of members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with those listed above;
- A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use or disclosure is being sought. If an expedited review procedure is used, the review and approval of the waiver or alteration of authorization may be carried out by the chair of the privacy board or by one or more members as designated by the chair.
- The documentation of the alteration or waiver of authorization must be signed by the chair, or other member as designated by the chair, of the IRB or privacy board, as applicable.

Attachment 15: Requirements for Uses and Disclosures to Avert a Serious Threat to Health or Safety.

A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

- Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
- Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat;
- Is necessary for law enforcement authorities to identify or apprehend an individual:
 - Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, or
 - Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody (as those terms are defined in the regulation).

A covered entity may NOT use or disclose information pursuant a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, if the information is learned

- In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or
- Through a request by the individual to initiate or to be referred for the treatment, counseling or therapy to affect the propensity to commit the criminal conduct involved.

Furthermore, a disclosure by a covered entity that is made because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, must be limited to:

- The information that was given in the statement made by the individual admitting participation in a violent crime; and
- The following: name and address; date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment; date and time of death, if applicable; and a description of distinguishing physical characteristics including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

The regulation describes the presumption of “good faith belief” as the belief being based upon the covered entity’s actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

Attachment 16: Requirements for De-identification of protected health information.

A covered entity may determine that health information is not individually identifiable health information only if:

- a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and method for rendering information not individually identifiable:
 - applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by and anticipated recipient to identify an individual who is a subject of the information, and
 - documents the methods and results of the analysis that justify such determination; or
- The following identifiers of the individual or of relatives, employers, or household members of the individual are removed:
 - Names;
 - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
 - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and
 - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000;
 - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
 - Telephone numbers;
 - Fax numbers;

- Electronic mail addresses;
- Social Security Numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers ;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URL);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code; and
- The covered entity does not have actual knowledge that the information could be used alone or in combination with other information, to identify an individual who is a subject of the information.

Attachment 17: Implementation Specifications for Minimum Necessary Uses of Protected Health Information.

For any type of disclosure that a covered entity makes on a routine and recurring basis, the entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, a covered entity must:

- Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and
- Review requests for disclosure on an individual basis in accordance with such criteria.

A covered entity may rely, if it is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

- Making disclosures to public officials as permitted under “uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required” (164.512);
- The information is requested by another covered entity;
- The information is requested by a professional who is a member of the entity’s workforce or is a business associate for the purpose of providing professional services, if the professional represents that the information requested is the minimum necessary for the stated purpose(s);
- Documentation or representations that comply with the applicable requirements for use and disclosure for research purposes (164.512(i)) have been provided by a person requesting the information for research purposes.

When a covered entity requests PHI from another covered entity, it must limit the request to that PHI which is reasonably necessary to accomplish the purpose for which the request is made. Furthermore,

- If the request is made on a routine and recurring basis, a covered entity must implement policies and procedures that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.
- If the request is not routine or recurring, a covered entity must review the request on an individual basis to determine that the PHI sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

For all uses, disclosures, or other requests to which the minimum necessary requirement applies, a covered entity may NOT use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Attachment 18: Requirements for Use and Disclosure of PHI for Marketing Purposes

A covered entity is not required to obtain an authorization when it uses or discloses PHI to make a marketing communication to an individual when the communication:

- Occurs in a face-to-face encounter with the individual;
- Concerns products or services of nominal value; or
- Concerns the health related products and services of the covered entity or of a third party and the communication meets the applicable conditions listed below.

A covered entity may disclose PHI for purposes of such communications only to a business associate that assists the covered entity with such communications.

The marketing communications must meet the following conditions:

- The communication must:
 - Identify the covered entity as the party making the communication;
 - Prominently state the fact that the covered entity has or will receive direct or indirect remuneration for making the communication, if that is the case; and
 - Except when the communication is contained in a newsletter or similar type of general communication device that the covered entity distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications.
- If the covered entity uses or discloses PHI to target the communication to individuals based on their health status or condition:
 - The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and
 - The communication must explain why the individual has been targeted and how the product or service relates to his/her health.

- The covered entity must also make reasonable efforts to ensure that individuals who decide to opt out of receiving future communications are not sent such communications.

Attachment 19: Requirements for Use and Disclosure of PHI for Fundraising Purposes

A covered entity is not required to obtain an authorization when it uses or discloses limited PHI to a business associate or to an institutionally related foundation for the purpose of raising funds for its own benefit. The PHI that is allowed to be disclosed is limited to:

- Demographic information relating to an individual; and
- Dates of health care provided to the individual.

Furthermore, the covered entity is only allowed to disclose such information if:

- A statement is included in the covered entity's notice of privacy practices for protected health information that the covered entity may contact the individual to raise funds for the covered entity;
- A description of how to opt out of receiving any further fundraising communications is included in the fundraising materials sent to the individual;
- The covered entity makes reasonable efforts to ensure that individuals who decide to opt out of receiving future communications are not sent such communications.

Attachment 20: Implementation Specifications for Verification

If a disclosure is conditioned on particular documentation, statement, or representations from the person requesting the PHI, a covered entity may rely (if such reliance is reasonable under the circumstances) on documentation, statements, or representations that on their face, meet the applicable requirements. Furthermore,

- The conditions for disclosures for law enforcement purposes pursuant to an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.
- The documentation required to show approval of an alteration or waiver for use or disclosure for research purposes may be satisfied by one or more written statements, provided that each is appropriately signed and dated in accordance with the regulation (see Attachment 14).

To verify the identity of public officials or persons acting on the behalf of public officials, for purposes of disclosing PHI, a covered entity may rely on (if such reliance is reasonable under the circumstances) any of the following:

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- If the request is in writing, the request is on the appropriate government letterhead; or

- If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

To verify the authority of public officials or persons acting on behalf of public officials, for purposes of disclosing PHI, a covered entity may rely on (if such reliance is reasonable under the circumstances) any of the following:

- A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority.
- If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

The verification requirements are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with the requirements for uses and disclosures requiring an opportunity for the individual to agree or to object (164.510), or acts of good faith belief in making a disclosure in accordance with the requirements of uses and disclosures for law enforcement purposes for which consent, authorization, or opportunity to agree or object is not required (164.512(j)).

Attachment 21: Access to Protected Health Information: Right of Access, Unreviewable Grounds for Denial, and Reviewable Grounds for Denial.

Individuals have a right of access to inspect and obtain a copy of PHI about themselves in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
- PHI that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access would be prohibited by law, or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

A covered entity may deny access without providing the individual an opportunity to review, in the following circumstances:

- The protected health information is excepted from right to access;
- An inmate's request to obtain PHI, if obtaining such information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate;
- Access to PHI that was created or obtained by the covered provider in the course of research that includes treatment may be temporarily suspended for as long as the

research is in progress, provided the individual has agreed to denial of access when consenting to participate in the research, and the provider has informed the individual that right to access will be reinstated upon completion of the research.

- If the PHI is contained in records subject to the Privacy Act, 5 U.S.C. 552a, access may be denied if the denial under the Privacy Act would meet the requirements of law.
- If the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

A covered entity may deny access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny, in the following circumstances:

- A licensed health care professional has determined, by professional judgment, that the access is reasonably likely to endanger the life or physical safety of the individual or another person;
- The PHI makes reference to another person (unless the person is a licensed health care professional) and a licensed health care professional, by professional judgment, had determined that access is reasonably likely to cause substantial harm to such person; or
- The request for access is made by the individual's personal representative, and a licensed health care professional, by professional judgment, had determined that access is reasonably likely to cause substantial harm to the individual or another person.

The covered entity must provide or deny access in accordance with the determination of the designated reviewing official.

A covered entity may require individuals to make requests for access in writing, provided it informs individuals of such a requirement.

Attachment 22: Conditions for Timely Action to Requests for Access

Except as provided below, a covered entity must act on a request for access no later than 30 days after receipt of the request as follows:

- If the request is granted, in whole or part, the covered entity must inform the individual of acceptance and provide the access requested in accordance with the conditions listed below;
- If the request is denied, in whole or part, the covered entity must provide the individual with a written denial in accordance with the criteria in Attachment 24;
- If the request is for PHI that is not maintained or accessible to the entity on-site, the entity must inform the individual of acceptance and provide the access requested no later than 60 days from the receipt of such request.
- If the covered entity is unable to grant or deny the request and inform the individual within 30 days of receipt of the request, the covered entity may extend the time for such actions by no more than 30 days, provided that:

- The covered entity provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and
- The covered entity may only have one such extension of time on a request for access.

Attachment 23: Requirements for Provision of Access

When the covered entity provides access, in whole or in part, to requested health information, the covered entity must comply with the following requirements:

- The entity must provide the access requested by the individual, including inspection or obtaining a copy, or both.
- If the information is maintained in more than one designated record set or at more than one location, the entity need only produce the PHI once in response to the request.
- The entity must provide the access in the form or format requested by the individual, if it is readily producible in such form or format, if not, in a readable hard copy form or other such format as agreed to be the entity and the individual;
- The entity may provide the individual a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided if:
 - The individual agrees in advance to such summary or explanation;
 - The individual agrees in advance to the fees imposed, if any, by the entity for the summary or explanation;
- The entity must provide the access as requested in a timely manner (see Attachment 22), including arranging with the individual a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy at the individual's request.
- The entity may discuss the scope, format, and other aspects of the request with the individual as necessary to facilitate the timely provision of access.
- The covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
 - Copying, including the cost of supplies for and labor of copying;
 - Postage, when the individual has requested the copy, summary, or explanation be mailed; and
 - Preparing an explanation or summary of the PHI, if agreed to by the individual as stated above.

Attachment 24: Requirements for Denial of Access

When the covered entity denies access, in whole or in part, to PHI, the covered entity must comply with the following requirements:

- The entity must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the entity has a ground to deny access;
- The entity must provide a timely (see Attachment 22), written denial to the individual;
- The denial must be in plain language and contain:
 - The basis for the denial;

- If applicable, a statement of the individual's review rights, including a description of how the individual may exercise such review rights; and
- A description of how the individual may complain to the covered entity (as specified in the notice of privacy practices) or to the Secretary. The description must include the name, or title, and telephone number of the contact person or office.
- If the entity does not maintain the PHI that is the subject of the request, and knows where the information is maintained, the entity must inform the individual where to direct the request for access.
- If the individual requests a review for denial, the entity must promptly refer the review request to the designated reviewing official.
 - The designated reviewing official must determine, within a reasonable period of time, whether or not to deny access based on the standards (see Attachment 21) for reviewable grounds for denial.
 - The entity must promptly provide written notice to the individual of the determination of the reviewing official and take other action as required to carry out the designated reviewing official's determination.

Attachment 25: Amendment of Protected Health Information

An individual has the right to have a covered entity amend 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. A covered entity may deny the request, if it determines that the PHI or record that is subject to the request:

- Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- It is not part of the designated record set;
- Would not be available for inspection (see information about access to PHI & records), or
- Is accurate and complete.

A covered entity may require individuals to make requests for amendment in writing, and to provide a reason to support a requested amendment, provided it informs individuals of such requirements.

Attachment 26: Requirements for Timely Action in Response to Requests for Amendment

A covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows:

- If the entity grants the requested amendment, in whole or in part, it must take actions required for making the amendment and informing the individual;
- If the entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial in accordance with the requirements for denying the amendment;

- If the entity is unable to act on the amendment within 60 days of receipt of the request, the entity may extend the time for such action by no more than 30 days, provided that:
 - The entity, within the initial 60 days, provides the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request; and
 - The entity may have only one such extension on a request for amendment.

Attachment 27: Requirements for Denial of a Request for Amendment

When the covered entity denies a requested amendment, in whole or in part, the covered entity must comply with the following requirements:

- The entity must provide the individual with a timely, written denial. The denial must use plain language and contain:
 - The basis for the denial
 - The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
 - A statement that, if the individual does not submit a statement of disagreement, the individual may request that the entity provide the individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
 - A description of how the individual may complain to the covered entity (following the complaint process in the notice) or to the Secretary. The description must contain the name or title, and telephone number of the contact person or office.

Attachment 28: Right to an Accounting of Disclosures of Protected Health Information

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

- To carry out treatment, payment, and health care operations;
- To individuals of PHI about them as provided in 164.502;
- For the facilities directory or to persons involved in the individual's care or other notification purposes;
- For national security or intelligence purpose;
- To correctional institutions or law enforcement officials; or
- That occurred prior to the compliance date for the covered entity.
- The entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides a written statement that such an accounting would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
- If the agency or official statement of above is made orally, the entity must:

- Document the statement, including the identity of the agency or official making the statement;
- Temporarily suspend the individual's right to receive and accounting of such disclosures;
- Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

An individual may submit a request for an accounting of disclosures for a time period less than six years from the date of the request.

Attachment 29: Content of the Accounting

The covered entity must provide the individual with a written accounting that meets the following requirements:

- Except as otherwise provided for in Attachment 28, the accounting must include disclosures of PHI that occurred during the six years (or shorter at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity;
- The accounting must include for each disclosure:
 - The date of the disclosure;
 - The name of the entity or person who received the PHI, and if known, the address of such entity or person;
 - A brief description of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or in lieu of such statement:
 - A copy of the individual's written authorization pursuant to uses and disclosures for which an authorization is required (164.508), or
 - A copy of a written request for disclosure when required by the Secretary to investigate or determine the entity's compliance with the regulation (164.502(a)(2)(ii)), or for uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required (164.512), if any.
- If during the period covered by the accounting, the covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose because it was required by the Secretary to investigate or determine compliance with the regulation (164.502(a)(2)(ii)), or for uses or disclosures for which consent, authorization, or opportunity to agree or object is not required (164.512), or pursuant to a single authorization under uses and disclosures for which an authorization is required (164.508), the accounting may, with respect to such multiple disclosures provide:
 - The information required for the first disclosure during the accounting period;
 - The frequency, periodicity, or number of disclosures made during the accounting period; and
 - The date of the last such disclosure during the accounting period.

Attachment 30: Provisions of the Accounting

The covered entity must act on the individual's request for an accounting no later than 60 days after receipt of such a request as follows:

- The entity must provide the individual with the accounting requested;
- If unable to provide the accounting requested within the 60 days, the entity may extend the time to provide the accounting by no more than 30 days, provided that:
 - The entity provides the individual, within the initial 60 days, with a written statement of the reasons for the delay and the date by which the accounting will be provided; and
 - The entity may only have one extension of time for action on a request for an accounting.
- The entity must provide the first accounting to an individual in any 12 month period without charge. However, the covered entity may:
 - Impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period; and
 - The entity informs the individual in advance of the fee; and
 - Provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Attachment 31: Policies and Procedures and Changes to Policies or Procedures

A covered entity must implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or the requirements of the regulation. The policies and procedures must be reasonably designed, taking into account the size and type of activities that relate to PHI by the covered entity, to ensure compliance.

A covered entity must make changes to its policies and procedures

- As necessary and appropriate to comply with changes in the law, including the standards, requirements and implementation specifications of the regulation;
- When a change in privacy practice effects a privacy practice that is described in the notice.

An entity may make other changes at any time, provided that the changes are documented and implemented in accordance with the requirements of the regulation.

To implement a policy and procedure change due to a change in law:

- Promptly document and implement the revised policy or procedure;
- Promptly make revisions to the notice, if the changes materially effects the content.

To implement revisions practices stated in the notice, a covered entity must:

- Ensure that the revised policy or procedure complies with the standards, requirements, and implementation specifications of the regulation;
 - Document the policy or procedure as revised;
 - Revise the notice as required to state the changed practice and make the notice available in accordance with the regulation. A change may not be implemented prior to the effective date of the revised notice.
- If a covered entity has not reserved the right to change a privacy practice that is stated in the notice, the entity may only make a change to a privacy practice that is stated in the notice if:
 - The change meets the implementation requirements noted above; and

- o Such change is effective only with respect to PHI created or received after the effective date of the notice.
- If a change to a policy or procedure does not materially effect the content of the notice:
 - o The policy or procedure must comply with the standards, requirements, and implementation specifications of the regulation;
 - o The change is documented as required, prior to the effective date of the change.

Checklist: Notice of Information

Use the following checklist to help with the development of a Notice of Information
The notice must contain the following elements:

- The following statement in the 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 the covered entity is permitted to make (by the regulation) for each of the following purposes: treatment, payment, and health care operations.
- A description of each of the other purposes for which the covered entity is permitted or required by the regulation to use or disclose protected health information without the individual’s written consent or authorization.
- If a use or disclosure for any purpose described in the above two items is prohibited or materially limited by law, the description of such use or disclosure must reflect the more stringent law as “more stringent” is defined in the regulation (see 160.202 of the regulation for the definition).
- For each purpose described in the second and third items listed above, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this regulation or other applicable law.
- 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 a covered entity intends to engage in any of the following activities the description of the types of uses and disclosures that the entity is permitted to make for treatment, payment, or health care operations, must include a separate statement (as applicable) that:

- The covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;
- The covered entity may contact the individual to raise funds for the covered entity; or
- A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose PHI to the sponsor of the plan.

The notice must contain a statement of the individual’s rights with respect to PHI and a brief description of how the individual may exercise these rights, as follows:

- The right to request restrictions on certain uses and disclosures of PHI as provided by the rights to request privacy protection for health information (164.522), including a statement that the covered entity is not required to agree to a requested restriction.
- The right to receive confidential communications of PHI (that meet the requirements for confidential communications found in 164.522(b)).

- The right to inspect and copy PHI (as provided by the regulation under access of individuals to protected health information (164.524)).
- The right to amend protected health information (as provided by the regulation (164.424)).
- The right to receive an accounting of disclosures of protected health information (as provided by the regulation (164.528)); and
- The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with the regulation (165.520(c)(3)), to obtain a paper copy of the notice from the covered entity upon request.

The notice must also contain statements relating to the covered entity's duties. This portion of the notice must contain:

- A statement that the covered entity is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI;
- A statement that the covered entity is required to abide by the terms of the notice currently in effect; and
- For the covered entity to apply a change in its privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with the regulation (164.530(i)(2)(ii)), a statement that it 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.

The notice must contain statements about complaint processes, contacts, and effective dates. These statements should contain the following information:

- A statement that individuals may complain to the covered entity or 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,
- 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 (as required by 164.530(a)(1)(ii))
- 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.

In addition to the elements and information required in the notice, a covered entity may include the following:

- If a covered entity elects to limit the uses or disclosures that it is permitted to make, a description of its more limited uses or disclosures, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

- For the covered entity to apply a change in its more limited uses and disclosures of PHI created or received prior to issuing a revised notice, the notice must include the statements that it 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.

Health plans must meet the following requirements when implementing their notice:

- Provide notice no later than the compliance date for the health plan, to individuals covered by the plan;
- Thereafter, at the time of enrollment, to individuals who are new enrollees; and
- Within 60 days of a material revision to the notice, to individuals then covered by the plan.
- No less frequently than every three years, notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

The above requirements are satisfied if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents. Furthermore, if the plan has more than one notice, it meets the above requirements by providing the notice that is relevant to the individual or other person requesting the notice.

Covered health care providers that have a direct treatment relationship with an individual must also meet the following requirements when implementing their notice:

- Provide notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider;
- Have the notice available at the service delivery site for individuals to take with them, (if the provider has a physical service delivery site); and
- Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the provider to be able to read the notice; and
- Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the above requirements for availability and posting, if applicable.

If the covered entity maintains a web site that provides information about the covered entity's customer services or benefits then the entity must:

- Prominently post its notice on the web site and make the notice available electronically through the web site.

An entity may provide the notice by e-mail if the individual agrees to electronic notice and the agreement has not been withdrawn. However,

- If the entity knows that the transmission has failed, a paper copy of the notice must be provided to the individual.
- Provision of electronic notice will satisfy the requirements of provision of notice if made timely in accordance with the specific requirements for health plans or health care providers that have a direct treatment relationship with an individual.

- Also, if the first service delivery to an individual is delivered electronically, an electronic notice must be provided automatically and contemporaneously in response to the individual's first request for service.
- Furthermore, the individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice, upon request.

Conditions for joint notice by separate covered entities that participate in an organized health care arrangement. A joint notice may be used provided that:

- The covered entities participating in the arrangement agree to abide by the terms of the notice with respect to PHI created or received as part of participation in the arrangement;
- The joint notice contains all the required elements, except that the statements may be altered to reflect that fact that the notice covers more than one entity; and
- Describes with reasonable specificity the covered entities, or class of entities, to which the notice applies;
- Describes with reasonable specificity the service delivery sites, or classes of sites, to which the notice applies; and
- If applicable, states that the covered entities participating in the arrangement will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the arrangement.
- The covered entities must provide the notice to individuals in accordance with all applicable implementation specifications noted in the above sections.

Provision of the joint notice to an individual by any of the entities included in the notice will satisfy provision of notice requirements for all other entities covered by the joint notice.