

Guide to Understanding HIPAA Privacy
An Instructional Document Written by WorkSmart MD, Inc.
Extracted from the HIPAA Rx™ Compliance Software

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated that the Department of Health and Human Services (DHHS) develop high-level health information security and privacy standards to support the increased use of electronic patient information contained as part of the standardized transactions. The final rules for the electronic transactions were published August 17, 2000, with compliance expected October 16, 2003. The final HIPAA privacy rule was published August 14, 2002 and became law on April 14, 2003. The privacy standards apply to “Covered Entities”: healthcare providers, payers and clearinghouses.

The intent of this instructional document on the final HIPAA privacy standards is to educate the reader by providing a breakdown of the various subsections of the regulations. For the purposes of this document HIPAA privacy rule or HIPAA privacy regulations refer the HIPAA privacy regulations 45 CFR 164.

Covered Entities

“Covered entities” include health plans, healthcare clearinghouses and healthcare providers. Examples of types of healthcare provider organizations that will be required to comply with HIPAA regulations include, but are not restricted to, the following:

- Physicians
- Chiropractors
- Dentists
- Hospitals
- Long-term care facilities
- Ambulatory care centers
- Pharmacies
- Home health agencies

Business Associates

Covered entities may disclose protected health information (“PHI”) to a business associate (such as billing contractors, transcriptionists, software vendors who have access to patient data, marketing and development firms, etc.) and may allow the business associate to create, maintain, or receive information on its behalf providing the covered entity has obtained “satisfactory assurances” that the business associate will safeguard the protected health information. Covered entities must document the satisfactory assurances through a written business associate contract. As part of the contract, there must be directions to business associates and subcontractors regarding use and disclosure as well as, at the termination of the contract, the return or destruction of protected health

information. Covered entities must create a process to respond to and resolve known privacy breaches by their business associates, or otherwise become responsible for the known actions.

Protected Health Information

The regulation defines protected health information (PHI) as individually identifiable information that is created, maintained or transmitted in any form – electronic, written or oral. On the other hand, the rules do not apply to information that has been de-identified by removing, encoding, or encrypting the individually identifiable health information. There are eighteen data elements that have been specifically identified for removal from a record for these purposes. When de-identifying information, organizations must make reasonable efforts to ensure that information needed for re-identification is not disclosed.

Patient's Rights to Privacy

The HIPAA privacy rule extends certain privacy rights and confidentiality protection to all patients regarding the confidentiality of their medical records and health information. The HIPAA privacy rule provides patients with the following rights:

- Covered entities must obtain permission from the patient before releasing health information for purposes other than treatment, payment, or healthcare operations.
- Patients must be provided a Notice of Privacy Practices that explains their privacy rights.
- Patients must be provided the right to request restrictions on the uses and disclosures of their health information.
- Patients must be permitted to request an accounting of health information disclosures.
- Patients must be able to access and copy their health information, except in certain situations.
- Patients must be permitted to request that they receive confidential communications regarding their health information.
- Patients must be provided the right to request amendments to their health information.

Covered entities must implement policies and procedures to facilitate patient's right to access their health information. Patients should be required to make all requests in writing.

Authorization for the Use and Disclosure of Health Information

When health information is being used for purposes other than treatment, payment or healthcare operations, an authorization for disclosure must be obtained from the patient.

To support this process and help patients in realizing their right to an accounting of information disclosure, covered entities should develop methods to track record access and disclosure. The regulation is very specific in defining information uses and disclosures that require authorization and those that do not.

Information Disclosures Requiring Authorization

The final HIPAA privacy rule contains a number of examples of situations that require authorization for the use or disclosure of protected health information. Specific rules exist regarding the authorization for the use of information contained in psychotherapy notes as well as the use of information for research purposes. In these instances, the regulations clearly address when authorizations would be considered valid and which would be deemed defective.

A valid authorization would contain at least the following core elements:

- Description of information to be used or disclosed
- Name of the person(s) authorized to use or disclose the information
- Name of the person(s) requesting the information
- Expiration date or event that relates to the information use or disclosure
- Statement of the individual's right to revoke the authorization and the exceptions to this right
- Statement that the authorized information may be subject to re-disclosure by the recipient and no longer protected by the authorization
- Signature of the individual and date
- Description of the personal representative's authority, if so needed

The regulations go further to define additional elements that would be required when a covered entity is requesting the information for its own use as well as requests made for disclosures by others.

Information Disclosure without Authorization

The privacy rule recognizes certain specific instances where individual authorization is not necessary. Examples of such permitted disclosures include:

- When required by law
- When needed for public health activities
- When information relates to a situation of abuse, neglect or domestic violence
- When needed for health oversight activities
- When required for judicial and administrative proceedings
- When required for law enforcement purposes
- When needed for cadaveric organ, eye or tissue donation purposes
- For research purposes
- For specialized government functions such as military and veterans activities
- For workers' compensation activities

The regulation adopts the Common Rule that currently governs federally funded research. Specifically, the researcher must either receive authorization from the patient or apply to the Institution's Review Board (IRB) for permission to use protected information without authorization. The IRB guidelines are very detailed, requiring the IRB's waiver to address eight (8) separate statements documenting their consideration. These statements include the risk, the rights of the individual, the need for the information and the adequacy of the plan to de-identify the information as soon as possible, and the assurance that the information will not be reused.

When information is being disclosed, the privacy regulation defines strict standards with respect to the type and amount of information disclosed. Organizations have to ensure that information is de-identified in accordance with the legislation, and that only the minimal amount of information needed is disclosed.

De-Identification of Protected Health Information

Health information may be used without authorization if it is de-identified by the covered entity. There are eighteen identifiers that have been specified in the regulation that must be removed for a record to be considered de-identified and void of any individually identifiable health information. Examples of information that must be removed to de-identify protected health information include: name(s) of the individual, relatives, employers and household members; specific demographic data smaller than a State; age; and contact information such as phone numbers, email address, SSN, account and medical record numbers, IP address, photographs, and biometric identifiers.

In some cases, the covered entity may determine that some demographic information may be left in the record, as long it is clearly not enough to identify the patient. An individual who has appropriate knowledge of statistical methods to determine the probability that the information cannot be individually identified must make this determination.

Minimum Necessary

The HIPAA privacy rule holds covered entities to a clear standard regarding the amount of data that may be revealed for specific purposes. Specifically, when a covered entity uses, discloses or requests protected health information, it must make reasonable effort to limit the amount to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

It is in this section of the regulations that marketing is covered. With some limitations, marketing activities may occur without authorization, provided the marketing activity:

- Occurs face-to-face with the individual
- Concerns products or services of nominal value
- Concerns the health-related products and services of the covered entity

Covered entities must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of a face-to-face communication made by a covered entity to an individual or a promotional gift of nominal value provided by the covered entity. If the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

Notice of Privacy Practices

The HIPAA privacy regulations state that the individual has a right to notice of the covered entities privacy practices and its legal obligation to respect the individual's rights. The regulations specifically define the content of such notice, for example that it must contain a description of the types and uses and disclosures that are permitted for the purposes of treatment, payment and health care operations; a description of other reasons that the covered entity may use or disclose information without authorization; and a statement of disclosures that may be made only with the individual's written authorization. In addition, the notice must specifically identify the individual's rights to privacy as discussed in an earlier section of this white paper. The August 14, 2002 final rule requires covered entities to obtain written acknowledgement from patients that they have reviewed the Notice of Privacy Practices, or, have documented the reason written acknowledgement was not obtained.

Administrative Procedures

Every covered entity must designate a privacy official who will be responsible for overseeing the development of policies and procedures that:

- Provide administrative, technical and physical safeguards to protect private information
- Establish and guide the office and individual who will receive and act on complaints of breach of privacy
- Ensure the collection of authorization from patients for the use of private information
- Provide notice to patients of their rights and the organization's obligation to protect those rights
- Train the workforce
- Establish sanctions for privacy violation by employees
- Mitigate, to the extent possible, the deleterious effects of privacy breaches

As has been the consistent with other parts of the HIPAA privacy regulations, implementation specifications are defined that must be followed by all covered entities.

Preemption of State Law

The HIPAA privacy rule states that if any of its terms are contrary to the state law, the HIPAA privacy rule will prevail. Additionally, the legislation states that any individual or state may request an exception to that part of the regulation. The HIPAA privacy rule further states that if the state law is more stringent than a federal standard, the state law will prevail. The new regulatory scheme should therefore be considered to constitute a “floor”, allowing states to add onto or deepen federally mandated protection(s).

Enforcement and Penalties

The Office of Civil Rights (OCR) of the Department of Health and Human Services (DHHS) will enforce the HIPAA privacy regulations. In order to ensure compliance by all covered entities, the Secretary of DHHS has implemented provisions that set forth enforcement actions including the investigation of complaints filed against covered entities, as well as the conducting of compliance reviews to assess compliance of covered entities. HIPAA permits the imposition of civil penalties of \$100 for each violation, and any one person may be fined up to \$25,000 per year. Criminal penalties may also be imposed on any person who knowingly uses or discloses protected health information inappropriately. Penalties for this type of infraction include fines ranging from \$50,000 to \$250,000 and up to 10 years imprisonment. It will be the responsibility of the organization to ensure that prudent measures are taken to protect privacy through the implementation of the required practices, supporting policies and procedures, and training activities that will minimize organizational risk to such investigations and penalties.

This break-down of the HIPAA privacy requirements provides an outline of the core elements and actions for each subpart of the HIPAA privacy regulations.

Uses & Disclosures for which an authorization is required - §164.508

Core Elements of an Authorization are: A specific description of the information to be disclosed, the name or other specific identification of the person(s) making the request, expiration date, a statement of the individual's right to revoke, statement that information used or disclosed may be subject to re-disclosure, signature and date, if signed by a representative a description of the authority.

Action: Specify intended use of PHI in authorization forms. Indicate in the document that authorizations go beyond release of information for purposes other than payment, treatment, and health care operations. Where applicable, indicate in the authorization form examples of intended uses PHI and what circumstances an authorization is required, for example disclosure of psychotherapy notes.

Minimum Necessary -§164.502(b) §164.514(d)

A covered entity must limit use and disclosure of PHI to the minimum necessary to carry out the intended purpose of the request.

Clarification: Minimum necessary does not apply to disclosures between providers in the context of treatment.

Action: Update employee policies that disclose PHI, such as for claims payment, limited distribution only to information related to a specific treatment. Use actual examples from payers to train employees on minimum necessary requirements.

Disclosures to Business Associates - §164.502(e)

Disclosures of PHI may be made to business associates where a Business Associate Contract is in place.

Clarification: Business Associate Contracts are not necessary between providers treating an individual.

Action: Revise existing vendor agreements to explain privacy standard requirements when using PHI. Request trading partners sign a Business Associate Agreement, i.e., medical labs and medical transcribers.

Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object - §164.510

PHI may be disclosed by a Covered Entity without the individual's authorization when used for facility directories (for clergy and other visitors), or to update family members

and individuals involved in the individual's care.

Clarification: Individuals must be given the opportunity to prohibit or restrict certain disclosures of PHI.

Action: Update Notice of Privacy Practices documentation to state that facilities may disclose limited PHI but must allow the patient an opportunity to object under limited situations. Examples of certain situations are: listing a patient's name in facility directory, blocking a family member from receiving information on health status, or for disaster relief purposes.

Uses and Disclosures for which an authorization or opportunity to agree or object is not required - §164.512(a) – (l)

A covered entity may use or disclose protected health information without the written authorization of the individual in the following circumstances:

- (a) Uses and disclosures required by law
- (b) Uses and disclosures for public health activities
- (c) Disclosures about victims of abuse, neglect or domestic violence
- (d) Uses and disclosures for health oversight activities
- (e) Disclosures for judicial and administrative proceedings
- (f) Disclosures for law enforcement purposes
- (g) Uses and disclosures about decedents
- (h) Uses and disclosures for cadaveric organ, eye or tissue donation purposes
- (i) Uses and disclosures for research purposes
- (j) Uses and disclosures to avert a serious threat to health or safety
- (k) Uses and disclosures for specialized government functions
- (l) Disclosures for workers' compensation

Clarification: The regulations provide methods by which these uses and disclosures maybe conducted. These uses and disclosures are limited and are outlined in detail in the regulations. The regulations give considerations to entities acting in good faith to protect the privacy rights of individuals when disclosing PHI for these purposes

Action: Develop detailed policies outlining each of these uses and disclosures with elements necessary for compliance. Include in Notice of Privacy Practices the organizations practices for permitting identified uses and disclosures.

De-identification of PHI - §164.514(a)

Individual health information loses its HIPAA protections and may be used or disclosed freely if it cannot be used to identify an individual.

Clarification: To be considered "de-identified," the health information cannot contain any of the nineteen specific identifiers of the individual and his/her relatives, employers,

or household members. However, it is possible that, even if one or more identifiers remain, information can still be treated as de-identified if a qualified statistician determines that the risk of identification is very small.

The nineteen identifiers are:

1. Name
2. All address information
3. E-mail addresses
4. Dates (except year)
5. Social Security Number
6. Medical record numbers
7. Health plan beneficiary numbers
8. Account numbers
9. Certificate numbers
10. License numbers
11. Vehicle identifiers
12. Facial photographs
13. Telephone numbers
14. Device identifiers
15. URLs
16. IP addresses
17. Biometric identifiers
18. The geographic unit formed by combining all zip codes with the same three initial digits containing more than 20,000 people and the initial three digits of all geographic units with fewer than 20,000 people is changed to 000.
19. 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

Action: Implement a release of information policy that requires senior level authorization on de-identified health information. Develop a checklist with the eighteen identifiers for de-identifying PHI data to be used for verification when preparing de-identifiable data files.

Notice of Privacy Practices for PHI - §164.520

Covered entities must provide individuals with Notice of Privacy Practices.

Clarification: The notice must be in “plain language” and include the following:

- (1) Information regarding uses and disclosures of PHI
- (2) Clarification of an individual’s privacy rights
- (3) The covered entity’s responsibilities under HIPAA
- (4) How to file complaints with the covered entity or Secretary of HHS
- (5) The name, title, and phone number of a contact person for more information and

(6) The effective date of the notice. A provider that has a direct treatment relationship with the individual must provide the notice no later than the date of the first service delivery (including services delivered electronically).

The notice must be available at the service delivery site for distribution upon request and posted in a prominent location. Providing an electronic notice satisfies the privacy practices notice requirement. Covered entities that are part of organized health care arrangements may use a joint notice. Covered entities must retain copies of the notices issued for six years.

Action: Openly display the Notice of Privacy Practices in patient waiting areas. Give Notice of Privacy Practices to each patient at time of office visit or as part of admission process and have patients acknowledge in writing that they have received this notice.

Rights to Request Privacy Protection for PHI - §164.522(a)

A covered entity must allow an individual to request that the covered entity restrict (1) uses and disclosure for treatment, payment and health care operations and (2) disclosures permitted for involvement in the individual's care and notification purposes.

Clarification: The restriction must be properly documented and retained for six years. However, the covered entity is not required to agree to the restriction. If the covered entity agrees to the restriction, it must abide by it except in emergency situations. A covered entity may terminate its agreement to a restriction if the individual agrees to or request the termination of the restriction, or if the covered entity informs the individual that it is terminating the restriction.

Action: Carefully review uses and disclosure practices with the patient as part of the initial visit. Ask the patient to identify restrictions of PHI. Include language in the Notice of Privacy Practices that patients have the right to request in writing restrictions on the uses and disclosures of their PHI, and that the covered entity is not required to agree with a requested restriction.

Confidential Communications Requirements - §164.522(b)

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

Clarification: This standard permits individuals to receive communications of PHI from a covered health care provider or a health plan by an alternative means or at an alternative address.

Action: Verify contact information and address as part of scheduling office visits. Include a section for alternative contact information on patient registration form. Define the boundaries of "reasonable" in the Notice of Privacy Practices document by noting when

the office will provide health information to an alternative address or by an alternative means.

Access of Individuals to PHI - §164.524

The individual has a right to inspect and copy his or her PHI, in whole or in part, for as long as the covered entity maintains the information.

Clarification: Individuals do not have an automatic right to access

- (1) Psychotherapy notes
- (2) Information on a criminal, civil or administrative action or proceeding or
- (3) PHI that is maintained by a covered entity that is subject to or exempted from Clinical Laboratory Improvements Amendments (CLIA) to the extent the provision of access would be prohibited by law.

The covered entity must act on a request for access within 30 days of receiving the request if the information is maintained and accessible on-site or within 60 days otherwise. The covered entity may grant itself a 30-day extension if certain conditions are met. Under certain circumstances a covered entity may deny a request for access of the PHI. For example, when access would endanger the life or safety of the individual. In the event that request for access is denied, the covered entity must provide the individual an opportunity for review.

The covered entity must designate a health care professional who did not participate in the original denial to conduct the review. The review decision must be made in a reasonable period of time and written notice of the review decision must be provided to the individual. Fees may be charged for access to PHI to cover the cost of photocopying, mailing, and summary preparation. The covered entity may provide the individual with a summary of the PHI request if the individual agrees to advance to the summary and to the fees imposed. The covered entity must retain the designated record sets that are subject to access by individuals and the titles of persons or offices responsible for processing requests for six years.

Action: Include language in Notice of Privacy Practices that patients have the right to access their personal health information for the previous six years. Record patient requests for access to their medical records in patient's file. As part of initial visit, advise patients of the right to access their medical records and the associated costs of doing so.

Amending PHI - §164.526

An individual has the right to have a covered entity amend his or her PHI in a designated record set for as long as the covered entity maintains the information.

Clarification: A covered entity may deny the request for amendment if:

- (1) *The PHI was not created by the covered entity (unless the individual claims the*

originator of the PHI is no longer available to amend the PHI)

(2) The PHI is not part of the designated record set

(3) The PHI was not available for inspection or

(4) The PHI is accurate and complete.

The covered entity may require the individual to make the request for amendment in writing and provide the rationale for the request. The covered entity must act within 60 days of the request (with a possible 30-day extension similar to that described for access to PHI). If the request for amendment is granted, the covered entity must notify the individual that amendment was accepted and obtain the individual's identification of and agreement to inform relevant persons. The covered entity must make reasonable efforts to inform relevant persons. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual and the covered entity, including business associates. If the request for amendment is denied, the covered entity must provide the individual with a timely written notice. The notice must explain the reason for denial, the individual's right to submit a written statement of disagreement or to have the request for amendment included with future disclosures, and the individual's right to complain to the covered entity or the Secretary of HHS.

The covered entity may prepare a rebuttal statement to the individual's state of disagreement. A copy of the rebuttal statement must be provided to the individual.

Future disclosures of the PHI must include the statement of disagreement or request for amendment, the denial notice, and the rebuttal or summary of this information. If a covered entity informs another covered entity of a necessary amendment of PHI, the covered entity must amend the record. The covered entity must retain documentation for six years.

Action: Include patient's right to amend PHI in the Notice of Privacy Practices. Outline process for making such a request. Implement procedures requiring appropriate provider signatures to approve amendments to patient records or resolving disputes. Retain approval or denial documentation as part of the medical record.

Accounting of Disclosures of PHI - §164.528

An individual has the right to receive an accounting of the disclosures of their PHI made by the covered entity in the six years prior to the request, except for the following disclosures.

- (1) For payment, treatment, and health care operations
- (2) To the individual
- (3) For the facility's directory or to persons involved in the individual's care
- (4) For national security or intelligence purposes
- (5) To correctional institutions or law enforcement officials
- (6) Which occurred prior to the HIPAA compliance date

Clarification: The covered entity must act on the request for an account of disclosure within 60 days with possible 30-day extensions as was described for accessing PHI. The covered entity must provide individuals with the first accounting at no charge. For subsequent requests within the same 12 month period, the covered entity may charge a reasonable, cost-based fee. The covered entity must provide a written account of each specific disclosure that includes the date of the disclosure, the person to whom the information was disclosed, brief description of the disclosed information, or, in lieu of the summary, a copy of the authorization or request for disclosure

Action: Maintain records of all patient disclosures regarding PHI as part of the medical record. Include in the documentation the date, description, and to whom information was disclosed. Implement procedures to authenticate patient requests for accounting and disclosure of PHI. Incorporate the patient's rights to receive a disclosure log of their PHI for six years prior to the date on which the accounting is requested in the Notice of Privacy Practices.

Administration Personnel Designations - §164.530(a)

Covered entities must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity and a contact person or office to receive complaints and provide further information about the covered entity's privacy practices.

Clarification: One employee is to be designated to be responsible for overseeing the implementation of policies and procedures, including the Notice of Privacy Practices as well as the employee policies manual on HIPAA standards and to ensure HIPAA compliance.

Action: Identify a staff member with knowledge of the covered entity with authority to investigate complaints to fill the role of privacy official. Designate an individual to address privacy complaints. Two different individuals or one in the same can handle these roles.

Training - §164.530(b)

A covered entity must train members of its workforce about the entity's policies and procedures for PHI and document that training has been provided.

Clarification: Training must be completed: For each member of the covered entity's workforce by no later than the compliance date for the covered entity; and Thereafter, for each new member of the workforce, within a reasonable period of time following the date of hire; and within a reasonable period of time after a material change in the entity's privacy policies and procedure becomes effective.

Action: Identify policies and procedures relating to PHI. Determine appropriate personnel

for training. Request workforce sign documentation outlining items covered during training and place copy in employee personnel files. Conduct PHI training upon hire and refresher training annually. Request workforce sign a statement of completion at the end of refresher training and place in employee personnel files.

Safeguards - §164.530(c)

A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional use or disclosure, or violation of the requirements of the regulation.

Clarification: Assure that employees use logins and passwords to access health information and that computers are safely secured from unauthorized use.

Action: Determine level of PHI access needed by each member of the workforce to complete his or her job. Establish access levels to PHI using logins and passwords as determined by job duties. Include security awareness as part of initial employee training and refresher training programs. Add manual locks to unsecured cabinets or store PHI in a secure location. Train workforce to limit conversations regarding PHI to private locations.

Complaints to the Covered Entity - §164.530(c)

A covered entity must provide a process for individuals to make complaints concerning its policies and procedures or its compliance with its policies and procedures or the requirements of the regulation.

Clarification: The covered entity must document all complaints received and their disposition.

Action: Advise patients during the registration process of the procedure to file a complaint. Include steps to file a complaint in the Notice of Privacy Practices. Designate a member of the workforce as the contact person for receiving and documenting complaints.

Sanctions - §164.530 (e)

A covered entity must have and apply appropriate sanctions against its employees who fail to comply with the entity's privacy policies and procedures or the regulations.

Clarification: Sanctions are not to be applied in certain situations, i.e. disclosures by whistleblowers and workforce member crime victims or as intimidating or retaliatory acts.

Action: Specify in the employee policies manual the organization's policy for dealing

with privacy infractions. Review with employees upon hire and at refresher training.

Refraining from Intimidating or Retaliatory Acts - §164.530(g)

A covered entity may not intimidate, threaten, coerce, discriminate or retaliate against an individual.

Clarification: Action cannot be taken against an individual, who exercises any right or process established under the regulation, including: the filing of a complaint, testifying, assisting, or participating in an investigation, compliance review, or hearing. Individuals can choose not to participate in any act or practice made unlawful by the regulation, provided the individual or person has a good faith belief that the practice opposed is unlawful, and that the manner of the opposition is reasonable and does not involve a disclosure of PHI that in itself constitutes violation.

Action: Employee-training programs that clarify the philosophy of management surrounding compliance with the HIPAA privacy rule. Management must train employees to exercise sound decisions that adhere to existing policies and to feel safe reporting non-compliance matters to the privacy official.

Waiver of Rights - §164.530(h)

A covered entity may not require an individual to waive his or her right to file a complaint with the DHHS as a condition of treatment, payment, and enrollment in a health plan, or eligibility for benefits.

Clarification: Patient must be informed by the organization that they have the right to file complaints and that the filing of a complaint will not interfere with their health care.

Action: Include language in the Notice of Privacy Practices that patients will not be asked to waive their rights to file a complaint with the Department of Health & Human Services as a condition of treatment. Include contact information for the Office of Civil Rights in the Notice of Privacy Practices. ((866)–OCR-PRIV)

Policies and Procedures - §164.530(i)(1)

A covered entity must develop and implement policies and procedures relating to PHI that are designed to comply with the elements of the regulations.

Clarification: The policies and procedures must take into account the size of and the type of activities that relate to PHI undertaken by the covered entity.

Action: Develop policies and procedures specific to HIPAA privacy requirements. Maintain in an electronic document or a hard copy for easy access by employees. Privacy policies and procedures should be developed in a manner that takes into account the size of and type of activities that relate to PHI by the covered entity.

Changes to Policies or Procedures - §164.530(i)(2)

A covered entity must revise its policies and procedures as necessary and appropriate to comply with changes in the law or regulations, or when it changes a privacy practice that is stated in its notice of privacy practices.

Clarification: A covered entity must change policies and procedures as necessary to comply with changes in law.

Action: A role of the privacy official is to monitor changes in the law, include as part of their job responsibility the task of updating all relevant documentation, employee training documents, and re-train existing employees.

Changes to Privacy Practices Stated in the Notice of Privacy Practices - §164.530(i)(4)

If a covered entity has not reserved its right to change a privacy practice described in the notice, the covered entity is bound by the privacy practices stated in the notice with respect to PHI created or received while the notice is in effect.

Clarification: The covered entity may change a privacy practice stated in the notice without having reserved the right to do so, provided that the change meets the implementation requirements described in the section and the change is effective only for PHI created or received after the effective date of the notice.

Action: Include language in the Notice of Privacy Practices that the covered entity reserves the right to change a privacy practice and outline activities of the organization regarding implementing changes in the law or operation relative to PHI. Inform patients of substantial changes in the Notice of Privacy Practices as part of the registration process.

Documentation - §164.530(j)

A covered entity must maintain its policies and procedures in written or electronic form for six years from the date of creation of the policies and procedures, or from the date when the policies and procedures became effective, whichever is later.

Clarification: For any communication required by the regulation to be in writing, the covered entity must maintain a written or electronic copy as documentation.

Action: Store HIPAA policies in a central HIPAA compliance manual accessible to employees. Provide employees with a copy of the HIPAA policies annually. Where possible, set up policies and procedures in an electronic format. Index policies and procedures by versions to comply with the six year retention rule. Include in the covered entity's Notice of Privacy Practices that they reserve the right to make changes at any

time to the policies and procedures. Indicate how changes will be communicated to patients.

Retention Period - §164.530(j)(2)

A covered entity must retain documentation required by regulation for six years from the date of its creation or the date when it last was in effect, whichever is later.

Clarification: A covered entity must retain written and electronic documentation for six years.

Action: Include a purge date on all written and electronic documentation.

Prior Authorizations - §164.532 (a)

A covered entity may continue to use or disclose an individual's PHI with the individual's authorization prior to the compliance date of the regulation, even though the authorization does not strictly comply with the requirements for authorization.

Clarification: The covered entity must not make any use or disclosure that is expressly excluded from the authorization or other express legal permission obtained from the individual prior to the implementation date, and must comply with any limitations placed by the individual executing the document.

Action: Train workforce to understand what PHI information can be used or disclosed prior to the HIPAA implementation date as part of their initial training. Clearly outline changes relating to use and disclosure of PHI after the implementation date.

General Rule and Exceptions – State Law - §160.203

Conflicting state law is preempted.

Clarification: There are four exceptions to this general rule:

- (1) The Secretary determines that the state law, regulation, or rule is necessary to prevent fraud and abuse related to the provision of or payment for health care.
- (2) To ensure appropriate State regulations of insurance and health plans to the extent expressly authorized by statute or regulations
- (3) For State reporting on health care delivery or cost.
- (4) For purposes of serving a compelling need related to public health, safety, or welfare or if the Secretary determined that an intrusion into privacy is warranted as determined by the need.

The broadest of these exceptions is the exception for state laws that are “more stringent” than the regulation. A state law is more stringent when it:

- (1) Prohibits or restricts a use or disclosure that the regulation would permit

- (2) Grants greater rights of access or amendment to an individual's own PHI
- (3) Provides for a greater amount of information to be disclosed to an individual upon request
- (4) Requires more narrowly focused or limited authorization
- (5) Requires more detailed record keeping
- (6) Provides any other greater privacy protection.

Action: Familiarize all employees with current State Law. Train employees to recognize where existing state laws supersede these federal regulations when State Law provides greater protections for individuals.

Complaints to the Secretary of HHS - §160.306

Any person who believes that a covered entity is not complying with the applicable requirements of HIPAA may file a complaint with the Secretary of HHS.

Clarification: Complaints to the Secretary must be in writing or electronic and must include the covered entities contact information and the nature of the violation.

Action: Advise patients during the registration process of the right to file a complaint and the appropriate steps. Include a section in the Notice of Privacy Practices on complaints.

Requirements for Filing Complaints - §160.306(b)

A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless the time limit is waived by the Secretary for good cause shown.

Clarification: Patients and family members need to be advised on the time frame in which they are permitted to file a complaint with the Secretary of HHS and that the complaint must be in writing and must name the covered entity in question.

Action: Advise patients during the registration process of the right to file a complaint and the appropriate steps. Include a section in the Notice of Privacy Practices on complaints.

Responsibilities of Covered Entities: Provide Records and Compliance Reports - §160.310

Covered entities are required to keep records of HIPAA compliance and submit compliance reports in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of the regulations.

Clarification: All policies and procedures and all other documentation of compliance with HIPAA privacy standards are to be maintained in the event of a request by the Secretary of HHS.

Action: Develop a summary document that outlines HIPAA activities of the organization. Delegate the privacy officer as point of contact for privacy issues.

Responsibilities of Covered Entities: Cooperate with Complaint Investigations and Compliance Reviews - §160.310 (b)(c)

Requires a covered entity to cooperate with the Secretary in investigations or compliance review of policies, procedures, or practices of a covered entity.

Clarification: Organizations need to be prepared to provide accurate and updated documentation of all HIPAA privacy related policies, requests, use, and disclosures, etc. in the event that a patient files a complaint with the Secretary of HHS.

Action: Inform workforce during orientation of management's willingness to participate in HHS investigations. Clearly identify for the workforce on all organizational flow charts a privacy official and contact person for complaints, and requests for additional information.