TECHNICALHELP4U

'The Privacy Rule' 45 CFR Parts 160 & 164

Privacy Act 101

'The Privacy Rule' 45 CFR Parts 160 & 164

Table of Contents

Chapter 1

The HIPAA Privacy Act

The Privacy Rule, effective April 14, 2001, is the first comprehensive federal protection for the privacy of health information. This rule is widely supported by all segments of the health care industry and supports the objective of enhanced patient privacy in the health care system.

Most health plans and providers that are covered by the new rule must comply with these new requirements by April 14, 2003 and small health plans will have three full years under the law (April 14, 2004) to come into compliance.

As required by Congress, this rule applies to: Health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically, such as electronic billing and fund transfers. This law does not apply to employers, life insurance companies or public agencies that deliver social security or welfare benefits.

Violators of this regulation could be denied health care, pay heavy fines or even go to prison. The rule, which has the effect of law, gives enormous enforcement powers to the secretary of the Department of Health and Human Services.

Severe penalties may be imposed on anyone who refuses to go along with the federal government's privacy rule.

Those penalties may be applied to all providers of health services – including physicians, dentists, hospitals, clinics, nursing homes, pharmacies, home-care services and health-insurance plans.

They could face fines of as much as $250,000 and prison terms up to 10 years.

PATIENTS MUST UNDERSTAND THAT:

Section 164.506(b)(1) states that "a covered health-care provider may condition treatment on the provision by the individual of a consent under this section."

Section 164.506(b)(2) states that "a health plan may condition enrollment in the health plan on the provision by the individual of a consent under this section. ..."

WHAT EXACTLY MUST THE INDIVIDUAL CONSENT TO?

As defined in Section 164.506(a)(1), it is the patient's consent to the health-care provider's "using or disclosing protected health information to carry out treatment, payment or health-care operations."

THIS CONSENT DOES NOT ALLOW USE OR DISCLOSURE FOR ANY REASON OTHER THAN TPO! A SPECIFIC AUTHORIZATION FORM IS REQUIRED FOR SITUATIONS OTHER THAN TPO.

Enforcement penalties applying to this rule are covered by Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

WHAT IF I DON'T FOLLOW THIS NEW RULE?

Section 1176 of that law provides civil monetary penalties of up to $100 "per person per violation" and up to $25,000 "per person for violations of a single standard for a calendar year."

Things get a lot tougher in Section 1177. For anyone who "knowingly" violates the requirements of the "privacy" rule the penalties range from $50,000 to $250,000 and/or imprisonment from one to 10 years.

The Privacy Rule became effective April 14, 2001. Most health plans and health care providers that are covered by this new rule must comply by April 14, 2003. Small health plans have until April 14, 2004 to come into complience.

The rule creates national standards to protect individuals' medical records and other personal health information.

Key points are:

- Patients have more control over their health information

- Boundaries are set on the use and release of health records

- Violators are held accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.

- Accounts for situations of public responsibility requiring disclosure of certain forms of data. ie.. when needed to protect public health.

Patients are able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

1. Enables patients to find out how their information may be used and what disclosures of their information have been made.

2. Limits release of information to the minimum reasonably needed for the purpose of the disclosure.

3. Gives patients the right to examine and obtain a copy of their own health records and request corrections.

The average health care provider needs to:

Provide information to patients about their privacy rights and how their information can be used.

Adopt clear privacy procedures for its practice, hospital or plan.

Train employees so that they understand the privacy procedures.

Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.

Securing patient records containing individually identifiable health information so that they are not readily accessible by unauthorized individuals.

Privacy Training 101 {45 CFR 164.506 Consent}

Congress dictates that health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically follow these rules, unless they deliver social security or welfare benefits.

REMEMBER, The Privacy Rule establishes a federal requirement that most doctors, hospitals, or other health care providers obtain a patient's written consent before using or disclosing the patient's personal health information to carry out treatment, payment or health care operations (TPO).

PROVIDERS KEY POINTS:

* Patient consent is required before a covered health care provider that has a direct treatment relationship with the patient may use or disclose protected health information (PHI) for purposes of TPO (treatment, payment, heath care operations).

* Providers that have indirect treatment relationships with patients (ie.. laboratories performing services for physicians), health plans, and health care clearinghouses may use and disclose PHI for purposes of TPO without obtaining a patients consent. You may still obtain constent if desired.

* If a patient refuses to consent to the use or disclosure of their PHI to carry out TPO, the Health care provider may refuse to treat the patient.

- **A patient's written consent need only be obtained by a provider one time.**

  * The consent document may be brief and written in general terms. See our templates section for examples. At a minimum, it must inform the patient that information may be used and disclosed for TPO, state the patients rights to review the providers privacy notice, to request restrictions and to revoke consent, and be dated and signed by the individual or his/her representative.

  * For specific PHI disclosurers, a more specific document, an authorization is required. See templates at the end of this manual.

Please note that:

1. The patient may revoke in writing, except to the extent that the covered entity has taken action in reliance on the consent.

2. The patient may request restrictions on uses or disclosures of health information for TPO. The covered entity need not agree to the restriction requested, but is bound by any restriction to which it agrees.

3. A patient must be given a notice of the covered entitity's privacy practices and may review that notice prior to signing a consent.

ADMISTRATIVE KEY POINTS :

1. Keep the signed consent for 6 years or longer from the date it was last in effect. The privacy rule does not dictate the form in which these consents are to be retained by the covered entity. You may store them physically or electronically by the current rule.

2. Integrated entities may obtain one joint consent for multiple entities.

3. In the case of conflicting consent information, disclose information only in accordance with the most restrictive document. Always err on the side of not disclosing sensitive information.

Train your employees regarding your policies

Ensure everyone understands the Privacy Rule and your policies

Document all training

Get Authorization for all releases or disclosures of PHI unrelated to the immediate TPO at hand

Ensure your Privacy Manager is aware of any changes to the rules.

Privacy Training 101 {45 CFR 164.502(b) 164.514(d)}

Minimum Necessary

The rule requires you to take reasonable steps to limit the use or disclosure of, and requests for protected health information (PHI) to the minimum neccessary to accomplish the intended purpose. These provisions do not apply to:

* Disclosures to or requests by a health care provider for treatment purposes.
* Disclosures to the individual who is the subject of the information
* Use or disclosure made pursuant to an authorization requested by the individual.
* Use or discloser required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.
* Disclosure to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
* Uses of disclosures that are required by other law.

Your policies and procedures must clearly identify the persons or postions within the organization who need access to the information to carry out their job duties, the types of PHI needed, and the conditions appropriate to such access.

An example may be at a hospital:

"Our policies permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case by case review of each use is not required."

Where the entire medical record is necessary, the policies and procedures must state so explicitily and include a justification. We have included sample policies for you in our templates section.

The rule permits you to rely on the judgement of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted, but not required, when the request is made by:

* A public official or agency for a disclosure permitted under 164.512 (Research) of the rule.

* Another covered entity.

* A professional who is a workforce member or business associate of the covered entity holding the information.

* A researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

Privacy Training 101 {45 CFR 160.103, 164.501}

Oral Communications

The Privacy Rule applies to individually identifiable health information in all forms: electronic, written, oral, and any other.

Coverage of oral (spoken) information ensures that information retains protections when discussed or read aloud from a computer screen or a written document. If oral communications were not covered, any health information could be disclosed to any person, so long as the disclosure was spoken.

Covered entities must reasonably safeguard protected health information (PHI) - including oral information - from any intentional or unintentional use or disclosure that is in violation of the rule.

They must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. "Reasonably safeguard" means that covered entities must make reasonable efforts to prevent uses and disclosures not permitted by the rule. However, it is not reasonable to expect safeguards to guarantee the privacy of PHI from any and all potential risks.

Covered entities must have policies and procedures that reasonably limit access to and use of PHI to the minimum necessary given the job responsibilities of the workforce and the nature of their work. The minimum necessary standard does not apply to disclosures, including oral disclosures, among providers for treatment purposes.

Reasonable safeguards for privacy in oral communications:

* Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area.

* Avoiding using patients' names in public hallways and elevators.

* Add curtains or screens to areas where oral communications often occur between doctors and patients or among professionals treating the patient.

* Pharmacies could ask customers to stand a few feet back from a counter used for patient counseling.

Protection of patient confidentiality is an important practice build upon these codes of conduct to develop the reasonable safeguards required by the Privacy Rule.

Privacy Training 101 {45 CFR 160.103, 164.502(e) 164.514(e)}

Business Associates

The Privacy Rule applies only to health plans, health care clearinghouses, and certain health care providers.

If you require assistance from contractors and other businesses it is permitted to give protected health information (PHI) to these "business associates,"

Such disclosures are permitted only once satisfactory assurances that the business associate will use the information only for the purposes for which they were engaged by the covered entity and will safeguard the information from misuse, abiding by your privacy policy regading this information and that it is not for independent use by the business associate.

A business associate is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI.

A business associate is not a member of the health care provider, health plan, or other covered entity's workforce.

A health care provider, health plan, or other covered entity can also be a business associate to another covered entity.

The business associate requirements do not apply to covered entities who disclose PHI to providers for treatment purposes - for example, information exchanges between a hospital and physicians with admitting privileges at the hospital

Parents and Minors

The Privacy Rule provides individuals with certain rights with respect to their personal health information, including the right to obtain access to and to request amendment of health information about themselves. These rights rest with that individual, or with the "personal representative" of that individual. In general, a person's right to control protected health information (PHI) is based on that person's right (under state or other applicable law, e.g., tribal or military law) to control the health care itself.

Because a parent usually has authority to make health care decisions about his or her minor child, a parent is generally a "personal representative" of his or her minor child under the Privacy Rule and has the right to obtain access to health information about his or her minor child. This would also be true in the case of a guardian or other person acting in loco parentis of a minor.

There are exceptions in which a parent might not be the "personal representative" with respect to certain health information about a minor child. In the following situations, the Privacy Rule defers to determinations under other law that the parent does not control the minor's health care decisions and, thus, does not control the PHI related to that care.

EXCEPTIONS TO THE RULE:

1. When state or other law does not require consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service, the parent is not the minor's personal representative under the Privacy Rule.

2. When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the relevant services.

3. When a parent agrees to a confidential relationship between the minor and the physician, the parent does not have access to the health information related to that conversation or relationship.

4. When a physician (or other covered entity) reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

The Privacy Rule also states that it does not preempt state laws that specifically address disclosure of health information about a minor to a parent . This is true whether the state law authorizes or prohibits such disclosure. If a physician believes that disclosure of information about a minor would endanger that minor, but a state law requires disclosure to a parent, the physician may comply with the state law without violating the Privacy Rule.

Privacy Training 101 {45 CFR 164.501, 164.514(e)}

Health-Related Communications and Marketing

The Privacy Rule defines "marketing" as:
"a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service."

The Privacy Rule identifies activities that are not considered marketing under this definition.

In recommending treatments or describing available services, health care providers and health plans are advising us to purchase goods and services. To prevent any interference with essential treatment or similar health related communications with a patient, the rule identifies the activities as not subject to the marketing provision, even if the activity otherwise meets the definition of marketing.

It is not 'marketing' when it:

* Describes the participating providers or plans in a network. For example, a health plan is not marketing when it tells its enrollees about which doctors and hospitals are preferred providers, which are included in its network, or which providers offer a particular service.

* Describes the services offered by a provider or the benefits covered by a health plan. For example, informing a plan enrollee about drug formulary coverage is not marketing.

* Part of a provider's treatment of the patient and for the purpose of furthering that treatment. For example, recommendations of specific brand-name or over-the-counter pharmaceuticals or referrals of patients to other providers are not marketing.
Made in the course of managing the individual's treatment or recommending alternative treatment. For example, reminder notices for appointments, annual exams, or prescription refills are not marketing.

LIMITATIONS ON MARKETING COMMUNICATIONS

If a communication is marketing, a covered entity may use or disclose PHI to create or make the communication, pursuant to any applicable consent obtained under § 164.506, only in the following circumstances:

* It is a face-to-face communication with the individual.
For example, sample products may be provided to a patient during an office visit.

* It involves products or services of nominal value. For example, a provider can distribute pens, toothbrushes, or key chains with the name of the covered entity or a health care product manufacturer on it.

* It concerns the health-related products and services of the covered entity or a third party, and only if the communication:

* Identifies the covered entity that is making the communication. ie.. the source of these marketing calls or materials.

* States that the covered entity is being compensated for making the communication, when that is so.

* Tells individuals how to opt out of further marketing communications, with some exceptions as provided in the rule. The covered entity must make reasonable efforts to honor requests to opt-out.

* Explains why individuals with specific conditions or characteristics (e.g., diabetics, smokers) have been targeted, if that is so, and how the product or service relates to the health of the individual. The covered entity must also have made a determination that the product or service may be of benefit to individuals with that condition or characteristic.

For all other communications that are "marketing" under the Privacy Rule, the covered entity must obtain the individual's authorization to use or disclose PHI to create or make the marketing communication.

Disclosure of PHI for marketing purposes is limited to disclosure to business associates that undertake marketing activities on behalf of the covered entity. No other disclosure for marketing is permitted. Covered entities may not give away or sell lists of patients or enrollees without obtaining authorization from each person on the list. As with any disclosure to a business associate, the covered entity must obtain the business associate's agreement to use the PHI only for the covered entity's marketing activities.

Privacy Training 101 {45 CFR 164.501, 164.508(f), 164.512(i)}

Research

The Privacy Rule establishes the conditions under which protected health information (PHI) may be used or disclosed by covered entities for research purposes. A covered entity may always use or disclose for research purposes health information which has been de-identified.

The Privacy Rule also defines the means by which individuals/human research subjects are informed of how medical information about themselves will be used or disclosed and their rights with regard to gaining access to information about themselves, when such information is held by covered entities. Where research is concerned, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time, ensuring that researchers continue to have access to medical information necessary to conduct vital research. Currently, most research involving human subjects operates under the Common Rule and/or the Food and Drug Administration's (FDA) human subjects protection regulations, which have some provisions that are similar to, but more stringent than and separate from, the Privacy Rule's provisions for research.

While conducting research, researchers may create, use, and/or disclose individually identifiable health information. Under the Privacy Rule, covered entities are permitted to use and disclose PHI for research with individual authorization, or without individual authorization under limited circumstances set forth in the Privacy Rule.

To use or disclose PHI without authorization by the research participant, a covered entity must obtain one of the following:

* Documentation that an alteration or waiver of research participants' authorization for use/disclosure of information about them for research purposes has been approved by an Institutional Review Board (IRB) or a Privacy Board.

* Representations from the researcher, either in writing or orally, that the use or disclosure of the PHI is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any PHI from the covered entity, and representation that PHI for which access is sought is necessary for the research purpose.

* Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the PHI of decedents, that the PHI being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought.

A covered entity may use or disclose PHI for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board provided it has obtained documentation of all of the following:

1. A statement that the alteration or waiver of authorization was approved by an IRB or Privacy Board that was composed as stipulated by the Privacy Rule;

2. A statement identifying the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved.

3. A brief description of the PHI for which use or access has been determined to be necessary by the IRB or Privacy Board;

4. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as stipulated by the Privacy Rule; and the signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

5. A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the following eight 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 the 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; and
- There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required 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 subpart.

As you may have determined, it is quite simpler to get prior approval:

The Privacy Rule also permits covered entities to use and disclose PHI for research purposes when a research participant authorizes the use or disclosure of information about him or herself. Today, for example, a research participant's authorization will typically be sought for most clinical trials and some records research. In this case, documentation of IRB or Privacy Board approval of a waiver of authorization is not required for the use or disclosure of PHI.

To use or disclose PHI created from a research study that includes treatment (e.g., a clinical trial), additional research-specific elements must be included in the authorization form required under § 164.508, which describe how PHI created for the research study will be used or disclosed. For example, if the covered entity/researcher intends to seek reimbursement from the research subject's health plan for the routine costs of care associated with the protocol, the authorization must describe types of information that will be provided to the health plan. This authorization may be combined with the traditional informed consent document used in research

Privacy Training 101 {45 CFR 160.300, 164.512(b), 164.512(f)}

Restrictions on Government Access to Health Information

Under the Privacy Rule, government-operated health plans and health care providers must meet substantially the same requirements as private ones for protecting the privacy of individual identifiable health information. For instance, government-run health plans, such as Medicare and Medicaid, must take virtually the same steps to protect the claims and health information that they receive from beneficiaries as private insurance plans or health maintenance organizations (HMO). In addition, all federal agencies must also meet the requirements of the Privacy Act of 1974, which restricts what information about individual citizens - including any personal health information - can be shared with other agencies and with the public.

The only new authority for government involves enforcement of the Privacy Rule itself. In order to ensure covered entities protect patients' privacy as required, the rule provides that health plans, hospitals, and other covered entities cooperate with the Department's efforts to investigate complaints or otherwise ensure compliance. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the privacy protections and access rights for consumers under this rule.

Payment

As provided for by the Privacy Rule, a covered entity may use and disclose protected health information (PHI) for payment purposes. "Payment" is a defined term that encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and for a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

Determining eligibility or coverage under a plan and adjudicating claims;
Risk adjustments;
Billing and collection activities;
Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
Utilization review activities; and
Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

Chapter

2

Templates & Checklist

1. Appoint a Privacy Manager. A simple memo will do. Place this in the appointee's personnell file and in your new 'Privacy Compliance' file.
2. Determine your Privacy Policy
   What do you do with your paperwork, where does it go, who sees it?
3. Secure your information Are new locks needed, do you have passwords on files, have employees been trained?
4. Paperwork Trail Document all training and privacy/security improvements. Keep all relevent paperwork as required by law.

Privacy Policy in accordance with HIPAA

Date:

Company:

We collect protected health information for purposes of treatment, payment or health care operations. This data is protected by the Privacy Rule of April 14 2001 "Standards for Privacy of Individually Identifiable Health Information".

Our Privacy manager is:_____

Our employees have all been trained in our privacy practices and have received interactive training in the subject, specifically regarding the Privacy Rule.

All patients are required to review and sign our Consent form prior to treatment, except in an emergency, when we are required by law to treat an individual, or when there are substantial communication barriers. We use an Authorization form for permission to use specified protected health information (PHI) for specific purposes, other than treatment, payment or health care operations (TPO), or to disclose PHI to a third party specified by the individual.

Information in the patient file will only be disclosed in the course of treatment, payment or health care operations, unless a specific Authorization has been obtained. Information such disclosed will be the minimum amount required to accomplish the task.

The administrative staff, nurses and doctors will have complete access to the patient files. This access is required to complete (TPO). Patient files are under supervision when unlocked during business hours. After hours the files are locked by the administrative staff. All computer's with access to PHI are password protected.

(THIS IS A BAREBONES POLICY, YOU MAY WISH TO CONSIDER AND ADD THE FOLLOWING:
1.What personal information is collected
2.Whether the collection method is voluntary or involuntary
3.How you can access and change the information
4.How the information will be used
5.Who--such as third-party marketers--will have access
6.How privacy problems will be resolved
7.What security provisions have been made to protect the data

Patient Consent Form

In accordance with The Privacy Rule "Standards for Privacy of Individually Identifiable Health Information" of April 14, 2001 we are notifying you about your privacy rights. Information collected in the course of treatment, payment or health care operations (TPO) is governed by our Privacy Policy. A copy of our current Privacy Policy is available from our front desk for review.

You have the right to revoke consent in writing, except to the extent that we have taken action in reliance on the consent.

You may request, but we are not obligated to honor, restrictions on uses or disclosures of health information for purposes of TPO. We are bound by any restriction to which we agree.

Signing this form does not permit us to sell your name, disclose information to an employer for employment decisions or to disclose information for eligibility for life insurance.

You have the right to review our privacy practices prior to signing this consent.

_____ _____

Sign & Print Name Today's Date

Retain in patient file for a minimum of 6 years from date last in effect.

Patient Authorization Form

In accordance with The Privacy Rule "Standards for Privacy of Individually Identifiable Health Information" of April 14, 2001 we are requesting the Authorization to use or disclose protected health information. Please review and sign below:

I agree to the release of the following information:

-Patient X ray charts
-Treatment review
-Billing statements

To: XYZ Insurance company

For the purposes of coordination of health benefits between plans.

_____

Sign & Print Name Today's Date

Retain in patient file for a minimum of 6 years from date last in effect.

Employee Privacy Training

I _____ have completed the Privacy 101 training program, reviewed our privacy policy and understand that civil and criminal penalties can be imposed if I violate patients' privacy rights.

_____

Sign & Print NameDate

Retain in employment file

Resources

Office of Civil Rights - Privacy of Health Records Updates: http://www.hhs.gov/ocr/hipaa/whatsnew.html

Compliance Plan Extensions:: http://www.cms.hhs.gov/hipaa/hipaa2/ASCAForm.asp