My State law authorizes health care providers to report suspected child abuse to the State Department of Health and Social Services. Does the HIPAA Privacy Rule preempt this State law? The Privacy Rule permits covered health care providers and other covered entities to disclose reports of child abuse or neglect to public health authorities or other appropriate government authorities. More>>

Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard? The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are More>>

Do disease management, health promotion, preventive care, and wellness programs fall under the HIPAA Privacy Rule's definition of "marketing"? Generally, no. To the extent the disease management or wellness program is operated by the covered entity directly or by a business associate, communications about such programs are not marketing because they are about the covered entity's own health-related services. More>>

What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule? The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. More>>

Can a covered entity bypass obtaining an individual's authorization for a use or disclosure not permitted by the HIPAA Privacy Rule simply by informing individuals of the use or disclosure through its notice of privacy practices? A covered entity's notice is not a substitute for an individual's authorization. More>>

My State requires consent to use or disclose health information. Does the HIPAA Privacy Rule take away this protection? The Privacy Rule does not prohibit a covered entity from obtaining an individual's consent to use or disclose his or her health information and, therefore, presents no barrier to the entity's ability to comply with State law requirements. More>>

If a research subject revokes his or her authorization to have protected health information used or disclosed for research, does the HIPAA Privacy Rule permit a researcher/covered health care provider to continue using the protected health information already obtained prior to the time the individual revoked his or her authorization? Covered entities may continue to use and disclose protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. More>>

By establishing new waiver criteria and authorization requirements, hasn't the HIPAA Privacy Rule, in effect, modified the Common Rule?

http://search.hhs.gov/search?entqr=1&access=p&getfields=*&entsp=0&sort=date%3AD%... 8/28/2007
Where both the Privacy Rule and the Common Rule apply, both regulations must be followed. More>>

When does a covered entity have discretion to determine whether a research component of the entity is part of their covered functions, and therefore, subject to the HIPAA Privacy Rule? Privacy of Health Information/HIPAA Research Uses and Disclosures More>>

Must all small health plans comply with the Privacy Rule? Certain plans are specifically excluded from having to comply with the HIPAA Administrative Simplification requirements, including the Privacy Rule. More>>
Are providers required to make a minimum necessary determination to disclose to Federal or State agencies, such as the Social Security Administration (SSA) or its affiliated agencies, for individuals' applications for Federal or State benefits?

These disclosures must be authorized by an individual and, therefore, are exempt from the HIPAA Privacy Rule's minimum necessary requirements.

Is a covered entity required to prevent any incidental use or disclosure of protected health information?

The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards.

A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

The Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy.

Are physicians and doctor's offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others?

The HIPAA Privacy Rule does not prohibit covered entities from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual's privacy while engaging in these practices.

Can a pharmacist use protected health information to fill a prescription that was telephoned in by a patient's physician without the patient's written consent if the patient is a new patient to the pharmacy?

The pharmacist is using the protected health information for treatment purposes, and the HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

Are hospitals able to inform the clergy about parishioners in the hospital?

The HIPAA Privacy Rule allows this communication to occur, as long as the patient has been informed of this use and disclosure, and does not object.

My State law says I may provide information regarding an injured workers' previous condition, which is not directly related to the claim for compensation, to an employer or insurer if I obtain the workers' written release. Am I permitted to make this disclosure under the HIPAA Privacy Rule?

A covered entity may disclose protected health information where the individual's written authorization has been obtained, consistent with the Privacy Rule's requirements at 45 CFR 164.508.

I am a health care provider and my State law says I have to provide a workers' compensation insurer, upon request, with an injured workers' records that related to treatment or hospitalization for which compensation is being sought. Am I permitted to disclose the information required by my State law?

The HIPAA Privacy Rule permits a covered entity to disclose protected health information as necessary to comply with State law.

Are health care providers required to seek a prior authorization before discussing a product or service with a patient, or giving a product or service to a patient, in a face-to-face encounter?

In face-to-face encounters, the HIPAA Privacy Rule allows covered entities to give or discuss products or
services, even when not health-related, to patients without a prior authorization. More>>>

Can telemarketers obtain my health information and use it to call me to sell goods and services? Under the HIPAA Privacy Rule, a covered entity can share protected health information with a telemarketer only if the covered entity has either obtained the individual’s prior written authorization to do so, or has entered into a business associate relationship with the telemarketer for the purpose of m More>>>

Result Page Previous 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 Next
Is it marketing for an insurance plan or health plan to send enrollees notices about changes, replacements, or improvements to existing plans?
The HIPAA Privacy Rule excludes from the definition of "marketing," communications about replacements of, or enhancements to, a health plan. More>>

Must insurance agents that are business associates of a health plan seek a prior authorization before talking to a customer in a face-to-face encounter about the insurance company's other lines of business?
No. In the specific case of face-to-face encounters, the HIPAA Privacy Rule allows health plans and their business associates to market both health and non-health insurance products to individuals. More>>

When is an authorization required from the patient before a provider or health plan engages in marketing to that individual?
The HIPAA Privacy Rule expressly requires an authorization for uses or disclosures of protected health information for ALL marketing communications, except in two circumstances: More>>

Are prior authorizations required when a doctor or health plan distributes promotional gifts of nominal value?
In a specific exception, the HIPAA Privacy Rule allows covered entities to distribute items commonly known as promotional gifts of nominal value without prior authorization, even if such items are distributed with the intent of encouraging the receiver to buy the products or services. More>>

Is it marketing for a covered entity to describe the entities participating in a health care provider network or a health plan network?
The HIPAA Privacy Rule excludes from the definition of "marketing," communications by a covered entity to describe the entities participating in a health care provider network or a health plan network. More>>

Is our medical practice required to notify patients through the mail of any changes to our notice?
The HIPAA Privacy Rule does not require a covered health care provider to mail out its revised notice or otherwise notify patients by mail of changes to the notice. More>>

Are covered entities permitted to give individuals a "layered" notice?
Covered entities may use a "layered" notice to implement the HIPAA Privacy Rule's requirements, so long as the elements required by 45 CFR 164.520(b) are included in the document that is provided to the individual. More>>

Are health plans required to make a good faith effort to obtain from their enrollees a written acknowledgement of receipt of the notice?
Under the HIPAA Privacy Rule, only covered health care providers that have a direct treatment relationship with individuals are required to make a good faith effort to obtain the individual's acknowledgment of receipt of the notice. More>>

If I believe that my privacy rights have been violated, when can I submit a complaint?
By law, health care providers (including doctors and hospitals) who engage in certain electronic transactions, health plans, and health care clearinghouses, (collectively, "covered entities") have until April 14, 2003, to comply with the HIPAA Privacy Rule. More>>

If a health care provider chooses to obtain an individual's consent to use or disclose protected health information about them, does the provider also have to make a good faith effort to obtain the individual's acknowledgement of the notice?
The HIPAA Privacy Rule requires that a covered health care provider with a direct treatment relationship
with individuals make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider's notice, regardless of whether the provider also chooses to ob More>>

Result Page Previous 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 Next
Is a physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office? Plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician's office, so they do not meet the definition of a "business associate". More>>

When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative? In general, and as explained below, the Privacy Rule permits a covered health care provider (covered provider), without the individual's written authorization, to disclose protected health information to a medical device company representative (medical device company) More>>

Must a covered entity provide an accounting for disclosures if the only information disclosed to a public health authority is in the form of a limited data set? A covered entity is not required to provide an accounting for a disclosure where the only information disclosed is in the form of a limited data set, and the covered entity has a data use agreement with the public health authority receiving the information. More>>

Can the fact that a patient has been "treated and released," or that a patient has died, be released as part of the facility directory? The fact that a patient has been "treated and released," or that a patient has died, may be released as part of the directory information about the patient's general condition and location in the facility, provided that the other requirements at 45 CFR 164.510(a) also are followed. More>>

Can an Authorization be used together with other written instructions from the intended recipient of the information? A transmittal or cover letter can be used to narrow or provide specifics about a request for protected health information as described in an Authorization, but it cannot expand the scope of the Authorization. More>>

May a covered entity use or disclose a patient's entire medical record based on the patient's signed Authorization? Yes, as long as the Authorization describes, among other things, the information to be used or disclosed by the covered entity in a "specific and meaningful fashion," and is otherwise valid under the Privacy Rule. More>>

Is a copy, facsimile, or electronically transmitted version of a signed Authorization valid under the Privacy Rule? Under the Privacy Rule, a covered entity may use or disclose protected health information pursuant to a copy of a valid and signed Authorization, including a copy that is received by facsimile or electronically transmitted. More>>

May a covered entity disclose protected health information specified in an Authorization, even if that information was created after the Authorization was signed? Yes, provided that the Authorization encompasses the category of information that was later
created, and that the Authorization has not expired or been revoked by the individual. More>>

May a valid Authorization list categories of persons who may use or disclose protected health information, without naming specific individuals or entities?

Yes. One Authorization form may be used to authorize uses and disclosures by classes or categories of persons or entities, without naming the particular persons or entities. More>>

Does the Privacy Rule permit a covered entity to use or disclose protected health information pursuant to an Authorization form that was prepared by a third party?

A covered entity is permitted to use or disclose protected health information pursuant to any Authorization that meets the Privacy Rule's requirements at 45 CFR 164.508. More>>
What effect do the "marketing" provisions of the HIPAA Privacy Rule have on Federal or State fraud and abuse statutes?

Answer

The Privacy Rule makes it clear that nothing in the marketing provisions of the Privacy Rule are to be construed as amending, modifying, or changing any rule or requirement related to any other Federal or State statutes or regulations, including specifically anti-kickback, fraud and abuse, or self-referral statutes or regulations, or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations. Examples of such laws include the anti-kickback statute (section 1128B(b) of the Social Security Act), safe harbor regulations (42 CFR Parts 411 and 424), and HIPAA statute on self-referral (section 1128C of the Social Security Act). The definition of "marketing" is applicable solely to the Privacy Rule and the permissions granted by the Rule are only for a covered entity's use or disclosure of protected health information. In particular, although the Privacy Rule defines the term "marketing" to exclude communications to an individual to recommend, purchase, or use a product or service as part of the treatment of the individual or for case management or care coordination of that individual, such communication by a health care professional may violate the anti-kickback statute. Similar examples of pharmacist communications with patients relating to the marketing of products on behalf of pharmaceutical companies were identified by the Office of the Inspector General (OIG) as problematic in a 1994 Special Fraud Alert (December 19, 1994, 59 FR 65372). Other violations have involved home health nurses and physical therapists acting as marketers for durable medical equipment companies. Although a particular communication under the Privacy Rule may not require patient authorization because it is not "marketing," or may require patient authorization because it is "marketing" as the Rule defines it, the arrangement may nevertheless violate other statutes and regulations administered by the Department of Health and Human Services, Department of Justice, or other Federal or State agencies.
Are the HIPAA Privacy Rule's requirements regarding patient access in harmony with the Clinical Laboratory Improvements Amendments of 1988 (CLIA)?

Answer

Yes. The Privacy Rule does not require clinical laboratories that are also covered health care providers to provide an individual access to information if CLIA prohibits them from doing so. CLIA permits clinical laboratories to provide clinical laboratory test records and reports only to "authorized persons," as defined primarily by State law. The individual who is the subject of the information is not always included as an authorized person. Therefore, the Privacy Rule includes an exception to individuals' general right to access protected health information about themselves if providing an individual such access would be in conflict with CLIA.

In addition, for certain research laboratories that are exempt from the CLIA regulations, the Privacy Rule does not require such research laboratories, if they are also a covered health care provider, to provide individuals with access to protected health information because doing so may result in the research laboratory losing its CLIA exemption.

Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

Answer
No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.

What are a covered entity's obligations under the HIPAA Privacy Rule with respect to protected health information held by a business associate during the contract transition period?

Answer

During the contract transition period, covered entities must observe the following responsibilities with respect to protected health information held by their business associates:

- Make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity.

- Fulfill an individual's rights to access and amend his or her protected health information contained in a designated record set, including information held by a business associate, if appropriate, and receive an accounting of disclosures by a business associate.

- Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of an impermissible use or disclosure of protected health information by its business associate.

Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.
However, a covered entity is not required to obtain the satisfactory assurances required by the Privacy Rule from a business associate to which the transition period applies.

Of course, even during the transition period, covered entities still may only disclose protected health information to a business associate for a purpose permitted under the Rule and must apply the minimum necessary standard, as appropriate, to such disclosures.

Is a covered entity required to apply the HIPAA Privacy Rule's minimum necessary standard to a disclosure of protected health information it makes to another covered entity? 2004, deadline for small health plan compliance with the Privacy Rule impose any new or additional requirements on health plans that are already subject to compliance with the Privacy Rule?

Answer

Covered entities are required to apply the minimum necessary standard to their own requests for protected health information. One covered entity may reasonably rely on another covered entity's request as the minimum necessary, and then does not need to engage in a separate minimum necessary determination. See 45 CFR 164.514(d)(3)(iii). However, if a covered entity does not agree that the amount of information requested by another covered entity is reasonably necessary for the purpose, it is up to both covered entities to negotiate a resolution of the dispute as to the amount of information needed. Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with another covered entity making a
request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.

Are there Privacy Rule compliance deadlines in 2004?

Answer

Yes, there are two deadlines for compliance with the HIPAA Privacy Rule on April 14, 2004:

• "Small health plans" (health plans with annual receipts of $5 million or less), must be in compliance with the Privacy Rule; and

• Covered entities (including small health plans) must, where required, have in place with their business associates written contracts or arrangements that meet Privacy Rule requirements.

Small Health Plans. Small health plans that are subject to HIPAA received an additional year – until April 14, 2004 – to come into compliance with the Privacy Rule. See 45 CFR 164.534(b)(2). These small health plans should already be familiar with HIPAA and should have assessed their covered entity status, since they have also been subject to the requirements of the HIPAA Transactions and Code Set Standards since October 2003.

Plans that are self-administered and have fewer than 50 participants are excluded from HIPAA’s Administrative Simplification requirements. (See the Answer to the FAQ "Must all small health plans comply with the Privacy Rule?") The Department of Health and Human Services’ (HHS) "Am I a Covered Entity?" decision tool, available at the HHS Office for Civil Rights (OCR) website, http://www.hhs.gov/ocr/hipaa, and also at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp, helps entities determine whether they are health plans or other HIPAA covered entities. These materials, hundreds of FAQs, and a wide range of other guidance and materials to assist covered entities in complying with HIPAA and the Privacy Rule, are available at the OCR website.

Business Associate Agreements. As of April 14, 2004, whenever the Privacy Rule requires covered entities to have written contracts or other arrangements with their business associates, these documents must include
provisions that comply with Privacy Rule requirements. As modified in August, 2002, the Privacy Rule provided most covered entities with up to one additional year – or until April 14, 2004 – to amend written contracts or other written arrangements that existed prior to October 15, 2002, to meet the Rule’s business associate requirements. (Unless they renewed automatically, contracts or other written arrangements were not eligible for this transition period if they were renewed, modified or newly entered into on or after October 15, 2002.) See 45 CFR 164.532(d) and (e). To assist covered entities in meeting these requirements, OCR has published a Fact Sheet regarding compliance with the Privacy Rule’s business associate requirements, sample business associate contract provisions, and a number of related Answers to Frequently Asked Questions, all of which are available on the OCR website at http://www.hhs.gov/ocr/hipaa.

Is this the first time small health plans are required to comply with HIPAA?

Answer

No. If a plan falls within the definition of small health plan in 45 CFR §160.103, it was required to be compliant with the HIPAA Transactions and Code Sets Standards Rule on October 16, 2003. Small health plans must also be in compliance with the HIPAA Employer Identifier Rule as of August 1, 2005, the HIPAA Security Rule as of April 20, 2006, and the National Provider Identifier Rule as of May 23, 2008. The Department of Health and Human Services (HHS) will publish guidance regarding implementation of these other HIPAA rules as their compliance dates approach. Information regarding compliance with the non-privacy HIPAA rules is available on the HHS Centers for Medicare and Medicaid Services website at: http://www.cms.hhs.gov/hipaa/hipaa2. Information regarding compliance with the Privacy Rule is available on the HHS Office for Civil Rights website at: http://www.hhs.gov/ocr/hipaa.

As an employer, I sponsor a group health plan for my employees. Am I a covered entity under HIPAA?
Covered entities under HIPAA are health care clearinghouses, certain health care providers, and health plans. A "group health plan" is one type of health plan and is a covered entity (except for self-administered plans with fewer than 50 participants). The group health plan is considered to be a separate legal entity from the employer or other parties that sponsor the group health plan. Neither employers nor other group health plan sponsors are defined as covered entities under HIPAA.

Thus, the Privacy Rule does not directly regulate employers or other plan sponsors that are not HIPAA covered entities. However, the Privacy Rule does control the conditions under which the group health plan can share protected health information with the employer or plan sponsor when the information is necessary for the plan sponsor to perform certain administrative functions on behalf of the group health plan. See 45 CFR 164.504(f). Among these conditions is receipt of a certification from the employer or plan sponsor that the health information will be protected as prescribed by the rule and will not be used for employment-related actions.

The covered group health plan must comply with Privacy Rule requirements, though these requirements will be limited when the group health plan is fully insured. See the Answer to the FAQ "Is a fully insured health plan subject to all Privacy Rule requirements?" That question, hundreds of FAQs, and a wide range of other guidance and materials to assist covered entities in complying with HIPAA and the Privacy Rule, are available at the Department of Health and Human Services Office for Civil Rights website, http://www.hhs.gov/ocr/hipaa.

Are State, county or local health departments required to comply with the HIPAA Privacy Rule?

Answer

Yes, if a State, county, or local health department performs functions that make it a covered entity, or otherwise meets the definition of a covered entity they must comply with the HIPAA Privacy Rule. For example, a state Medicaid program is a covered entity (i.e., a health plan) as defined in the
Privacy Rule. Some health departments operate health care clinics and thus are health care providers. If these health care providers transmit health information electronically in connection with a transaction covered in the HIPAA Transactions Rule, they are covered entities. For more information, see the definitions of covered entity, health care provider, health plan and health care clearinghouse in 45 CFR 160.103. See also, the "Covered Entity Decision Tools" posted at http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

These tools address the question of whether a person, business or agency is a covered health care provider, health care clearinghouse or health plan. If the health department performs some covered functions (i.e., those activities that make it a provider that conducts certain transactions electronically, a health plan or a health care clearinghouse) and other non-covered functions, it may designate those components (or parts thereof) that perform covered functions as the health care component(s) of the organization and thereby become a type of covered entity known as a "hybrid entity." Most of the requirements of the Privacy Rule apply only to the hybrid entity's health care component(s). If a health department elects to be a hybrid entity, there are restrictions on how its health care component(s) may disclose protected health information to other components of the health department. See 45 CFR 164.103 and 164.105 for more information about hybrid entities.

Learn More: The HIPAA Law and Related Information: http://www.cms.hhs.gov/HIPAAgenInfo/02_TheHIPAALawandRelated%20Information.asp#TopOfPage

My State law provides greater privacy protections on patients' HIV information than the HIPAA Privacy Rule. Is this more protective State law preempted by the Privacy Rule?

Answer

No. The Privacy Rule establishes a floor of Federal privacy protections and rights for individuals. If a provision of State law provides greater privacy protection than a provision of the Privacy Rule, and it is possible to comply with both the State law and the Privacy Rule (e.g., where a State law
prohibits the disclosure of HIV status while the Privacy Rule permits such disclosure), there is no conflict between the State law and the Privacy Rule, and no preemption.

Further, even in the unusual case where a "more stringent" provision of a State law is "contrary" to a provision of the Privacy Rule – that is, it is impossible to comply with both the Privacy Rule and the State law, or the State law is an obstacle to accomplishing the full purposes and objectives of HIPAA's Administrative Simplification provisions – the Administrative Simplification Rules specifically provide an exception to preemption of State law. Thus, if a more stringent provision of State law protects HIV patient information and is contrary to the Privacy Rule, the "more stringent" State law would prevail. Because HIPAA's Administrative Simplification Rules themselves except more stringent, contrary State law from preemption, it is neither necessary nor appropriate to request a preemption exception determination from the Department of Health and Human Services. See 45 C.F.R. 160.202 for the definitions of "more stringent" and "contrary," and 45 C.F.R. 160.203 for the general rule and exceptions to preemption. An unofficial version of the Privacy Rule and the preemption requirements may be accessed at http://www.hhs.gov/ocr/combinedregtext.pdf (PDF - 2.8MB).
What does the HIPAA Privacy Rule do?

Answer

Most health plans and health care providers that are covered by the new Rule must comply with the new requirements by April 14, 2003.

The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site (http://www.hhs.gov/ocr/hipaa/) and our full set of Frequently Asked Questions.

Last revised: March 28, 2007
In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. When it comes to personal information that moves across hospitals, doctors’ offices, insurers or third party payers, and State lines, our country has relied on a patchwork of Federal and State laws. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient’s medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient’s application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new Federal privacy standards.

Health care providers have a strong tradition of safeguarding private health information. However, in today’s world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the Rule provides clear standards for the protection of personal health information.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

Answer

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating 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 available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the Rule to protect patients' privacy. Covered entities of all types and sizes are required to comply with the Privacy Rule. To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.
- The training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.
- The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
Who must comply with HIPAA privacy standards?

Answer

As required by Congress in HIPAA, the Privacy Rule covers:

- Health plans
- Health care clearinghouses
- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

These entities (collectively called "covered entities") are bound by the privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. The law does not give the Department of Health and Human Services (HHS) the authority to regulate other types of private businesses or public agencies through this regulation. For example, HHS does not have the authority to regulate employers, life insurance companies, or public agencies that deliver social security or welfare benefits. See the fact sheet and frequently asked questions about the standards on "Business Associates" for a more detailed discussion of the covered entities' responsibilities when they engage others to perform essential functions or services for them.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
When will covered entities have to meet these HIPAA privacy standards?

Answer

As Congress required in HIPAA, most covered entities have until April 14, 2003 to come into compliance with these standards, as modified by the August, 2002 final Rule. Small health plans will have an additional year – until April 14, 2004 – to come into compliance.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is providing assistance to help covered entities prepare to comply with the Rule. For example, OCR maintains a web site with helpful information, such as the Guidance, Frequently Asked Questions, sample "business associate" contract provisions, significant reference documents, and other technical assistance information for consumers and the health care industry, at http://www.hhs.gov/ocr/hipaa/.

Last revised: March 30, 2007
What were the major modifications to the HIPAA Privacy Rule that the Department of Health and Human Services (HHS) adopted in August 2002?

Answer

Based on the information received through public comments, testimony at public hearings, meetings at the request of industry and other stakeholders, as well as other communications, HHS identified a number of areas in which the Privacy Rule, as issued in December 2000, would have had potential unintended effects on health care quality or access. As a result, HHS proposed modifications that would maintain strong protections for the privacy of individually identifiable health information, address the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieve unintended administrative burdens created by the Privacy Rule.

Final modifications to the Rule were adopted on August 14, 2002. Among other things, the modifications addressed the following aspects of the Privacy Rule:

- Uses and disclosures for treatment, payment and health care operations, including eliminating the requirement for the individual's consent for these activities;

- The notice of privacy practices that covered entities must provide to patients;

- Uses and disclosures for marketing purposes;

- Minimum necessary uses and disclosures;

- Parents as the personal representatives of unemancipated minors;

- Uses and disclosures for research purposes; and

- Transition provisions, including business associate contracts.

In addition to these key areas, the modifications included changes to certain other provisions where necessary to clarify the Privacy Rule, and a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

For more information about the final modifications to the Privacy Rule, see the Fact Sheet entitled, Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule. This Fact Sheet can be found at http://www.hhs.gov/news/press/2002pres/20020809.html.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?

Answer

The consent requirement created the unintended effect of preventing health care providers from providing timely, quality health care to individuals in a variety of circumstances. The most troubling and pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care. The following are some examples of how the consent requirement would have posed barriers to health care:

- Pharmacists would not have been able to fill a prescription, search for potential drug interactions, determine eligibility, or verify coverage before the individual arrived at the pharmacy to pick up the prescription if the individual had not already provided consent under the Privacy Rule.

- Hospitals would not have been able to use information from a referring physician to schedule and prepare for procedures before the individual presented at the hospital for such procedure, or the patient would have had to make a special trip to the hospital to sign the consent form.

- Providers who do not provide treatment in person (such as a provider prescribing over the telephone) may have been unable to provide care because they would have had difficulty obtaining prior written consent to use protected health information at the first service delivery.

- Emergency medical providers were concerned that, even if a situation was urgent, they would have had to try to obtain consent to comply with the Privacy Rule, even if that would be inconsistent with the appropriate practice of emergency medicine.

- Emergency medical providers were also concerned that the requirement that they attempt to obtain consent as soon as reasonably practicable after an emergency would have required significant efforts and administrative burden which might have been viewed as harassing by patients, because these providers typically do not have ongoing relationships with individuals.

To eliminate such barriers to health care, mandatory consent was replaced with the voluntary consent provision that permits health care providers to obtain consent for treatment, payment and health care operations, at their option, and enables them to obtain consent in a manner that does not disrupt needed treatment. Although consent is no longer mandatory, the Rule still affords individuals the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded. These modifications will ensure that the Rule protects patient privacy as intended without harming consumers' access to care or the quality of that care. Further, the individual's right to request restrictions on the use or disclosure of his or her protected health information is retained in the

Rule as modified.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.

Last revised: March 28, 2007
Did the final modifications to the HIPAA Privacy Rule alter the compliance date(s) for covered entities?

Answer

No. The compliance dates for the Privacy Rule, as modified, remain April 14, 2003, for most health plans, covered health care providers, and health care clearinghouses, and April 14, 2004, for small health plans. Under HIPAA, compliance with a modification to an existing standard or implementation specification is required by a date set by the Secretary, but not earlier than 180 days from the adoption of the modification. By publishing the modifications to the Privacy Rule in August 2002, the original compliance date of April 2003 is maintained for the entire Rule, as modified.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
Will the Department of Health and Human Services (HHS) make future changes to the HIPAA Privacy Rule and, if so, how will these changes be made?

Answer

Under HIPAA, HHS has the authority to modify the privacy standards as the Secretary may deem appropriate. However, a standard can be modified only once in a 12-month period.

As a general rule, future modifications to the Privacy Rule must be made in accordance with the Administrative Procedure Act (APA). HHS will comply with the APA by publishing proposed rule changes, if any, in the Federal Register through a Notice of Proposed Rulemaking and will invite comment from the public. After reviewing and addressing those comments, HHS will issue a modified final rule.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

Answer

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers’ primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Health care staff may orally coordinate services at hospital nursing stations.

- Nurses or other health care professionals may discuss a patient’s condition over the phone with the patient, a provider, or a family member.

- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.

- A physician may discuss a patients’ condition or treatment regimen in the patient’s semi-private room.

- Health care professionals may discuss a patient’s condition during training rounds in an academic or training institution.

- A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

Answer

No, the Privacy Rule does not require these types of structural changes be made to facilities.

Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard.

For example, the Privacy Rule does not require the following types of structural or systems changes:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.
- Encryption of telephone systems.

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent health care and health information professionals are taking to protect patient privacy.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

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

- In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers may constitute a reasonable safeguard. For example, a large clinic intake area may reasonably use cubicles or shield-type dividers, rather than separate rooms, or providers could add curtains or screens to areas where discussions often occur between doctors and patients or
among professionals treating the patient.

- Hospitals could ensure that areas housing patient files are supervised or locked.

Last revised: April 03, 2007

May physicians offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?

Answer

Yes. Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

Last revised: April 03, 2007
Are physicians and doctor's offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others?

Answer:

No. The HIPAA Privacy Rule does not prohibit covered entities from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual's privacy while engaging in these practices. Covered entities must implement reasonable safeguards to protect an individual's privacy. In addition, covered entities must reasonably restrict how much information is used and disclosed, where appropriate, as well as who within the entity has access to protected health information. Covered entities must evaluate what measures make sense in their environment and tailor their practices and safeguards to their particular circumstances.

For example, the Privacy Rule does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual's privacy:

- Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., "high fall risk" or "diabetic diet") at patient bedside or at the doors of hospital rooms.

  Possible safeguards may include: reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.

- Announcing patient names and other information over a facility's public announcement system.

  Possible safeguards may include: limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.

- Use of X-ray lightboards or in-patient logs, such as whiteboards, at a nursing station.

  Possible safeguards may include: if the X-ray lightboard is in an area generally not accessible by the public, or if the nursing station whiteboard is not readily visible to the public, or any other safeguard which reasonably limits incidental disclosures to the general public.

The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.
A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the HIPAA Privacy Rule allow the clinic to continue this practice?

Answer

Yes, the Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient’s privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. (See 45 CFR 164.502(a)(1)(iii). As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary requirement would be satisfied. Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by. Each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances. See 45 CFR 164.530(c).
A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the HIPAA Privacy Rule allow the hospital to continue this practice?

**Answer**

The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure—for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. In this case, disclosure of patient names by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or health care operations purposes (for example, as a service for patients and their families). The disclosure of such information to other persons (such as other visitors) that will likely also occur due to the posting is an incidental disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate. See 45 CFR 164.502(a)(1)(iii). In this case, it would appear that the disclosure of names is the minimum necessary for the purposes of the permitted uses or disclosures described above, and there do not appear to be additional safeguards that would be reasonable to take in these circumstances. However, each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances.

Last revised: March 26, 2007
May mental health practitioners or other specialists provide therapy to patients in a group setting where other patients and family members are present?

Answer

Yes. Disclosures of protected health information in a group therapy setting are treatment disclosures and, thus, may be made without an individual's authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose protected health information to a family member or other person involved in the individual's care. Where the individual is present during the disclosure, the covered entity may disclose protected health information if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual's agreement to participate in group therapy or family discussions is a good basis for inferring the individual's agreement.
Are covered entities required to document incidental disclosures permitted by the HIPAA Privacy Rule, in an accounting of disclosures provided to an individual?

Answer

No. The Privacy Rule includes a specific exception from the accounting standard for incidental disclosures permitted by the Rule. See 45 CFR 164.528(a)(1).

Last revised: April 03, 2007
Do the HIPAA Privacy Rule's provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?

Answer

No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

- A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.

- A health plan employee discussing a patient's health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.
Is a covered entity required to prevent any incidental use or disclosure of protected health information?

Answer:

No. The HIPAA Privacy Rule does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Rule requires only that covered entities implement reasonable safeguards to limit incidental uses or disclosures. See 45 CFR 164.530(c)(2).
How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

Answer

The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.

The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.
Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

Answer

No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

Uses of protected health information for treatment are not exempt from the minimum necessary standard. However, the Privacy Rule provides the covered entity with substantial discretion with respect to how it implements the minimum necessary standard, and appropriately and reasonably limits access to identifiable health information within the covered entity. The Rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity may develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.
Do the HIPAA Privacy Rule’s minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patient medical information in the course of their training?

Answer

No. The definition of “health care operations” in the Privacy Rule provides for “conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers.” Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients’ medical information, including entire medical records.

Last revised: April 03, 2007
Must the HIPAA Privacy Rule's minimum necessary standard to be applied to uses or disclosure that are authorized by an individual?

Answer

No. Uses and disclosures that are authorized by the individual are exempt from the minimum necessary requirements. For example, if a covered health care provider receives an individual’s authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of 45 CFR 164.508.
May physician's offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?

Answer

Yes. The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual’s privacy, covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

A covered entity also may leave a message with a family member or other person who answers the phone when the patient is not home. The Privacy Rule permits covered entities to disclose limited information to family members, friends, or other persons regarding an individual’s care, even when the individual is not present. However, covered entities should use professional judgment to assure that such disclosures are in the best interest of the individual and limit the information disclosed. See 45 CFR 164.510(b)(3).

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, the Department considers a request to receive mailings from the covered entity in a closed envelope rather than by postcard to be a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances. See 45 CFR 164.522(b).
Are providers required to make a minimum necessary determination to disclose to Federal or State agencies, such as the Social Security Administration (SSA) or its affiliated agencies, for individuals' applications for Federal or State benefits?

Answer

No. These disclosures must be authorized by an individual and, therefore, are exempt from the HIPAA Privacy Rule’s minimum necessary requirements. Furthermore, use of the provider’s own authorization form is not required. Providers can accept an agency’s authorization form as long as it meets the requirements of 45 CFR 164.508 of the Privacy Rule.
Doesn't the HIPAA Privacy Rule minimum necessary standard conflict with the HIPAA transaction standards?

Answer

No, because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the transactions standards, including disclosures of all data elements that are required or situationally required in those transactions. See 45 CFR 164.502(b)(2)(vi). However, covered entities have significant discretion as to the information included in the transactions as optional data elements. Therefore, the minimum necessary standard does apply to the optional data elements. The transactions standard adopted for the outpatient pharmacy sector is an example of a standard that uses optional data elements. The health plan, or payer, currently specifies which of the optional data elements are needed for payment of its particular pharmacy claims. The health plan or its business associates must apply the minimum necessary standard when requesting this information. In this example, a pharmacist may reasonably rely on the health plan's request for information as the minimum necessary for the intended disclosure. For example, as part of a routine protocol, the name of the individual may be requested by the payer as the minimum necessary to validate the identity of the claimant or for drug interaction or other patient safety reasons.
Does the HIPAA Privacy Rule strictly prohibit the use, disclosure, or request of an entire medical record? If not, are case-by-case justifications required each time the entire medical record is disclosed?

Answer

No. The Privacy Rule does not prohibit the use, disclosure, or request of an entire medical record; and a covered entity may use, disclose, or request an entire medical record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures and requests would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes. The Privacy Rule does not require that a justification be provided with respect to each distinct medical record. Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment purposes or disclosures to the individual who is the subject of the protected health information.
A provider might have a patient's medical record that contains older portions of a medical record that were created by another previous provider. Will the HIPAA Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

Answer

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

Last revised: March 26, 2007
In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigning office space and upgrading computer systems, in order to comply with the HIPAA Privacy Rule's minimum necessary requirements?

Answer

No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to protected health information to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. In this case, appropriate training of employees may be sufficient. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the Privacy Rule.

Last revised: March 26, 2007
May a covered entity accept documentation of an external Institutional Review Board's (IRB) waiver of authorization for purposes of reasonably relying on the request as the minimum necessary?

**Answer**

Yes. The HIPAA Privacy Rule explicitly permits a covered entity to reasonably rely on a researcher's documentation of an Institutional Review Board (IRB) or Privacy Board waiver of authorization pursuant to 45 CFR 164.512(i) that the information requested is the minimum necessary for the research purpose. See 45 CFR 164.514 (d)(3)(ii). This is true regardless of whether the documentation is obtained from an external IRB or Privacy Board or from one that is associated with the covered entity.
Does the HIPAA Privacy Rule change the way in which a person can grant another person health care power of attorney?

Answer

No. Nothing in the Privacy Rule changes the way in which an individual grants another person power of attorney for health care decisions. State law (or other law) regarding health care powers of attorney continue to apply. The intent of the provisions regarding personal representatives was to complement, not interfere with or change, current practice regarding health care powers of attorney or the designation of other personal representatives. Such designations are formal, legal actions which give others the ability to exercise the rights of, or make treatment decisions related to, an individual. The Privacy Rule provisions regarding personal representatives generally grant persons, who have authority to make health care decisions for an individual under other law, the ability to exercise the rights of that individual with respect to health information.
If someone has health care power of attorney for an individual, can they obtain access to that individual's medical record?

Answer

Yes, an individual that has been given a health care power of attorney will have the right to access the medical records of the individual related to such representation to the extent permitted by the HIPAA Privacy Rule at 45 CFR 164.524. However, when a physician or other covered entity reasonably believes that an individual, including an unemancipated minor, has been or may be subjected to domestic violence, abuse or neglect by the personal representative, or that treating a person as an individual's personal representative could endanger the individual, the covered entity may choose not to treat that person as the individual's personal representative, if in the exercise of professional judgment, doing so would not be in the best interests of the individual.
Can the personal representative of an adult or emancipated minor obtain access to the individual's medical record?

Answer

The HIPAA Privacy Rule treats an adult or emancipated minor's personal representative as the individual for purposes of the Rule regarding the health care matters that relate to the representation, including the right of access under 45 CFR 164.524. The scope of access will depend on the authority granted to the personal representative by other law. If the personal representative is authorized to make health care decisions, generally, then the personal representative may have access to the individual’s protected health information regarding health care in general. On the other hand, if the authority is limited, the personal representative may have access only to protected health information that may be relevant to making decisions within the personal representative’s authority. For example, if a personal representative’s authority is limited to authorizing artificial life support, then the personal representative’s access to protected health information is limited to that information which may be relevant to decisions about artificial life support.

There is an exception to the general rule that a covered entity must treat an adult or emancipated minor’s personal representative as the individual. Specifically, the Privacy Rule does not require a covered entity to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. This exception applies to adults and both emancipated and unemancipated minors who may be subject to abuse or neglect by their personal representatives.
How can family members of a deceased individual obtain the deceased individual's protected health information that is relevant to their own health care?

**Answer**

The HIPAA Privacy Rule recognizes that a deceased individual's protected health information may be relevant to a family member’s health care. The Rule provides two ways for a surviving family member to obtain the protected health information of a deceased relative. First, disclosures of protected health information for treatment purposes—even the treatment of another individual—do not require an authorization; thus, a covered entity may disclose a decedent's protected health information, without authorization, to the health care provider who is treating the surviving relative. Second, a covered entity must treat a deceased individual’s legally authorized executor or administrator, or a person who is otherwise legally authorized to act on the behalf of the deceased individual or his estate, as a personal representative with respect to protected health information relevant to such representation. Therefore, if it is within the scope of such personal representative's authority under other law, the Rule permits the personal representative to obtain the information or provide the appropriate authorization for its disclosure.
Does the HIPAA Privacy Rule address when a person may not be the appropriate person to control an individual's protected health information?

Answer

Generally, no. The Rule defers to State and other laws that address the fitness of a person to act on an individual's behalf. However, a covered entity does not have to treat a personal representative as the individual when it reasonably believes, in the exercise of professional judgment, the individual is subject to domestic violence, abuse or neglect by the personal representative, or doing so would otherwise endanger the individual.
May personal representatives access health information based on a non-health care power of attorney?

Answer:

No. Except with respect to decedents, a covered entity must treat a personal representative as the individual only when that person has authority under other law to act on the individual's behalf on matters related to health care. A power of attorney that does not include decisions related to health care in its scope would not authorize the holder to exercise the individual's rights under the HIPAA Privacy Rule. Further, a covered entity does not have to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

With respect to personal representatives of deceased individuals, the Privacy Rule requires a covered entity to treat the personal representative as the individual as long as the person has the authority under law to act for the decedent or the estate. The power of attorney would have to be valid after the individual's death to qualify the holder as the personal representative of the decedent.
May adults with mental retardation control their protected health information if they are able to authorize uses and disclosures of their protected health information?

Answer

Individuals may control their protected health information under the HIPAA Privacy Rule to the extent State or other law permits them to act on their own behalf. Further, even if an individual is deemed incompetent under State or other law to act on his or her own behalf, covered entities may decline a request by a personal representative for protected health information if the individual objects to the disclosure (or for any other reason), and the disclosure is merely permitted, but not required, under the Rule.

However, covered entities must make disclosures that are required under the Rule (i.e., disclosures to the Secretary under subpart C of part 160 regarding enforcement of the Rule, and to the individual under 45 CFR 164.524 and 164.528 with respect to the individual’s right of access to his or her protected health information and an accounting of disclosures, respectively). Consequently, with respect to the individual’s right of access to protected health information and for an accounting of disclosures, covered entities must provide the individual’s personal representative access to the individual’s protected health information or an accounting of disclosures upon the request of the personal representative, unless the covered entity, in the exercise of professional judgment, believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. The Rule allows a specified time period before a covered entity must act on such a request; and during this interim period, an individual and his personal representative will have an opportunity to resolve any dispute they may have concerning the request.
How does a covered entity identify an individual's personal representative?

Answer

State or other law determines who is authorized to act on an individual's behalf, thus the Privacy Rule does not address how personal representatives should be identified. Covered entities should continue to identify personal representatives the same way they have in the past. However, the HIPAA Privacy Rule does require covered entities to verify a personal representative's authority in accordance with 45 CFR 164.514(h).

Last revised: March 26, 2007
Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?

Answer

Yes, the Privacy Rule generally allows a parent to have access to the medical records about his or her child, as his or her minor child's personal representative when such access is not inconsistent with State or other law.

There are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are:

1. When the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law;
2. When the minor obtains care at the direction of a court or a person appointed by the court; and
3. When, and to the extent that, the parent agrees that the minor and the health care provider may have a confidential relationship.

However, even in these exceptional situations, the parent may have access to the medical records of the minor related to this treatment when State or other applicable law requires or permits such parental access. Parental access would be denied when State or other law prohibits such access. If State or other applicable law is silent on a parent's right of access in these cases, the licensed health care provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

Finally, as is the case with respect to all personal representatives under the Privacy Rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child has been or may be subjected to domestic violence, abuse or neglect, or that treating the parent as the child's personal representative could endanger the child.

Last revised: April 03, 2007
If a child receives emergency medical care without a parent's consent, can the parent get all information about the child's treatment and condition?

Answer

Generally, yes. Even though the parent did not consent to the treatment in this situation, the parent would be the child's personal representative under the HIPAA Privacy Rule. This would not be so when the parent does not have authority to act for the child (e.g., parental rights have been terminated), when expressly prohibited by State or other applicable law, or when the covered entity, in the exercise of professional judgment, believes that providing such information would not be in the best interest of the individual because of a reasonable belief that the individual may be subject to abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual.

Last revised: March 26, 2007
Does the HIPAA Privacy Rule provide rights for children to be treated without parental consent?

Answer

No. The Privacy Rule does not address consent to treatment, nor does it preempt or change State or other laws that address consent to treatment. The Rule addresses access to, and disclosure of, health information, not the underlying treatment.

Last revised: April 03, 2007
When an individual reaches the age of majority or becomes emancipated, who controls the protected health information concerning health care services rendered while the individual was an unemancipated minor?

Answer

The individual who is the subject of the protected health information can exercise all rights granted by the HIPAA Privacy Rule with respect to all protected health information about him or her, including information obtained while the individual was an unemancipated minor consistent with State or other law. Generally, the parent would no longer be the personal representative of his or her child once the child reaches the age of majority or becomes emancipated, and therefore, would no longer control the health information about his or her child. Of course, any individual can have a personal representative – which may include a parent – who can exercise rights on his or her behalf.

Last revised: March 26, 2007
May a psychologist continue his practice to notify a parent before treating his or her minor child, even though the minor child is able to consent to such health care under State law?

Answer

The HIPAA Privacy Rule would defer to State or other applicable law that addresses the disclosure of health information to a parent about a minor child. If the minor child is permitted, under State law, to consent to such health care without the consent of her parent and does consent to such care, the provider may notify the parent when the State law explicitly requires or permits the health provider to do so. If State law permits the minor child to consent to such health care without parental consent, but is silent on parental notification, the provider would need the child’s permission to notify a parent.

Last revised: March 26, 2007
Has the Secretary exceeded the HIPAA statutory authority by requiring "satisfactory assurances" for disclosures to business associates?

Answer

No. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the Secretary authority to directly regulate health plans, health care clearinghouses, and certain health care providers. It also grants the Department explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by covered entities. Therefore, the Department does have the authority to condition the disclosure of protected health information by a covered entity to a business associate on the covered entity's having a written contract with that business associate.
Has the Secretary exceeded the HIPAA statutory by requiring "business associates" to comply with the Privacy Rule, even if that requirement is through a contract?

Answer

The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the covered entity comply with its obligations under the Rule.

Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of protected health information.
What are a covered entity's obligations under the HIPAA Privacy Rule with respect to protected health information held by a business associate during the contract transition period?

Answer:

During the contract transition period, covered entities must observe the following responsibilities with respect to protected health information held by their business associates:

- Make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity.
- Fulfill an individual's rights to access and amend his or her protected health information contained in a designated record set, including information held by a business associate, if appropriate, and receive an accounting of disclosures by a business associate.
- Mitigate, to the extent practicable, any harmful effect that is known to the covered entity of an impermissible use or disclosure of protected health information by its business associate.

Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.

However, a covered entity is not required to obtain the satisfactory assurances required by the Privacy Rule from a business associate to which the transition period applies.

Of course, even during the transition period, covered entities still may only disclose protected health information to a business associate for a purpose permitted under the Rule and must apply the minimum necessary standard, as appropriate, to such disclosures.
I have an existing contract with a business associate that will renew automatically before April 14, 2003. Does this automatic renewal mean I have to modify the contract by April 14, 2003, to make it compliant with the HIPAA Privacy Rule's business associate contract provisions or can I still take advantage of the transition period?

Answer

Evergreen or other contracts that renew automatically without any change in terms or other action by the parties and that exist by October 15, 2002, are eligible for the transition period. The automatic renewal of a contract itself does not terminate qualification for the transition period, or the transition period itself. Renewal or modification for the purposes of the transition provisions requires action by the parties involved. For example, an automatic inflation adjustment to the price of a contract does not trigger the end of the transition period, nor make the contract ineligible for the transition period if the adjustment occurs before April 14, 2003.
Is a covered entity liable for, or required to monitor, the actions of its business associates?

Answer

No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504 (e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

Last revised: April 03, 2007
Instead of entering into a contract, can business associates self-certify or be certified by a third party as compliant with the HIPAA Privacy Rule?

Answer

No. A covered entity is required to enter into a contract or other written arrangement with a business associate that meets the requirements at 45 CFR 164.504(e).

Last revised: April 03, 2007
Are accreditation organizations business associates of the covered entities they accredit?

Answer

Yes. The HIPAA Privacy Rule explicitly defines organizations that accredit covered entities as business associates. See the definition of "business associate" at 45 CFR 160.103. Like other business associates, accreditation organizations provide a service to the covered entity which requires the sharing of protected health information. The business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity. As an alternative to the business associate contract, covered entities may disclose a limited data set of protected health information, not including direct identifiers, to an accreditation organization, subject to a data use agreement. See 45 CFR 164.514(e). If only a limited data set of protected health information is disclosed, the satisfactory assurances required of the business associate are satisfied by the data use agreement.

Last revised: April 03, 2007
Is a business associate contract required for a covered entity to disclose protected health information to a researcher?

Answer

No. Disclosures from a covered entity to a researcher for research purposes do not require a business associate contract, even in those instances where the covered entity has hired the researcher to perform research on the covered entity's own behalf. A business associate agreement is required only where a person or entity is conducting a function or activity regulated by the Administrative Simplification Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103. However, the HIPAA Privacy Rule does not prohibit a covered entity from entering into a business associate contract with a researcher if the covered entity wishes to do so. Notwithstanding the above, a covered entity is only permitted to disclose protected health information to a researcher as permitted by Rule, that is, with an individual's authorization pursuant to 45 CFR 164.508, without an individual's authorization as permitted by 45 CFR 164.512(1), or as a limited data set provided that a data use agreement is in place as permitted by 45 CFR 164.514(e).
When is a health care provider a business associate of another health care provider?

Answer

The HIPAA Privacy Rule explicitly excludes from the business associate requirements disclosures by a covered entity to a health care provider for treatment purposes. See 45 CFR 164.502(e)(1). Therefore, any covered health care provider (or other covered entity) may share protected health information with a health care provider for treatment purposes without a business associate contract. However, this exception does not preclude one health care provider from establishing a business associate relationship with another health care provider for some other purpose. For example, a hospital may enlist the services of another health care provider to assist in the hospital’s training of medical students. In this case, a business associate contract would be required before the hospital could allow the health care provider access to patient health information.
May a covered entity share protected health information directly with another covered entity's business associate?

Answer

Yes. If the HIPAA Privacy Rule permits a covered entity to share protected health information with another covered entity, the covered entity is permitted to make the disclosure directly to a business associate acting on behalf of that other covered entity.

Last revised: April 03, 2007
Are covered entities that engage in joint activities under an organized health care arrangement (OHCA) required to have business associate contracts with each other?

Answer

No. Covered entities that participate in an OHCA are permitted to share protected health information for the joint health care activities of the OHCA without entering into business associate contracts with each other. Of course, each such entity is independently required to observe its obligations under the HIPAA Privacy Rule with respect to protected health information.

Last revised: April 03, 2007
Is a business associate contract required with organizations or persons where inadvertent contact with protected health information may result - such as in the case of janitorial services?

Answer

A business associate contract is not required with persons or organizations whose functions, activities, or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all. Generally, janitorial services that clean the offices or facilities of a covered entity are not business associates because the work they perform for covered entities does not involve the use or disclosure of protected health information, and any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the HIPAA Privacy Rule. See 45 CFR 164.502(a)(1).

If a service is hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity’s premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service.
Is a physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office?

Answer

No, plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician's office, so they do not meet the definition of a "business associate". Under the HIPAA Privacy Rule, "business associates" are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. See the definition of "business associate" at 45 CFR 160.103.

Any disclosure of protected health information to such technicians that occurs in the performance of their duties (such as may occur walking through or working in file rooms) is limited in nature, occurs as a by-product of their duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule. See 45 CFR 164.502(a)(1).
Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

Answer:

No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.
Does the HIPAA Privacy Rule require a business associate to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?

Answer

The Privacy Rule regulates covered entities, not business associates. The Rule requires covered entities to include specific provisions in agreements with business associates to safeguard protected health information, and addresses how covered entities may share this information with business associates. Covered entities are responsible for fulfilling Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting, as provided for by 45 CFR 164.524, 164.526, and 164.528. With limited exceptions, a covered entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must make such protected health information available if and when needed by the covered entity to provide an individual with access to the information. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the designated record set, or part thereof.

Under 45 CFR 164.526, a covered entity must amend protected health information about an individual in a designated record set, including any designated record sets (or copies thereof) held by a business associate. Therefore, the Rule requires covered entities to specify in the business associate contract that the business associate must amend protected health information in such records (or copies) when requested by the covered entity. The covered entity itself is responsible for addressing requests from individuals for amendment and coordinating such requests with its business associate. However, the Privacy Rule also does not prevent the parties from agreeing through the contract that the business associate will receive and address requests for amendment on behalf of the covered entity.

Under 45 CFR 164.528, the Privacy Rule requires a covered entity to provide an accounting of certain disclosures, including certain disclosures by its business associate, to the individual upon request. The business associate contract must provide that the business associate will make such information available to the covered entity in order for the covered entity to fulfill its obligation to the individual. As with access and amendment, the parties can agree through the business associate contract that the business associate will provide the accounting to individuals, as may be appropriate given the protected health information held by, and the functions of, the business associate.
Would business associate contracts in electronic form, with an electronic signature, satisfy the HIPAA Privacy Rule's business associate contract requirements?

Answer

Yes, assuming that the electronic contract satisfies the applicable requirements of State contract law. The Privacy Rule generally allows for electronic documents, including business associate contracts, to qualify as written documents for purposes of meeting the Rule's requirements. However, currently, no standards exist under HIPAA for electronic signatures. In the absence of specific standards, covered entities must ensure any electronic signature used will result in a legally binding contract under applicable State or other law.
Do physicians with hospital privileges have to enter into business associate contracts with the hospital?

Answer

No. The hospital and such physicians participate in what the HIPAA Privacy Rule defines as an organized health care arrangement (OHCA). Thus, they may use and disclose protected health information for the joint health care activities of the OHCA without entering into a business associate agreement.
Under the HIPAA Privacy Rule, may a covered entity contract with a business associate to create a limited data set the same way it can use a business associate to create de-identified data?

Answer:

Yes. See 45 CFR 164.514(e)(3)(ii). For example, if a researcher needs county data, but the covered entity’s data contains only the postal address of the individual, a business associate may be used to convert the covered entity’s geographical information into that needed by the researcher. In addition, the covered entity may hire the intended recipient of the limited data set as the business associate for this purpose in accordance with the business associate requirements. That is, the covered entity may provide protected health information, including direct identifiers, to a business associate who is also the intended data recipient, to create a limited data set of the information responsive to the recipient’s request. However, the data recipient, as a business associate, must agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.
I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data and use agreement and business associate contract?

Answer

Yes. A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule. In the above situation, because the covered entity is providing the recipient with protected health information that includes direct identifiers, a business associate agreement would be required in addition to the data use agreement to protect the information. For example, the agreement must require that the recipient agree to return or destroy the information that includes the direct identifiers once it has completed the conversion for the covered entity.

Last revised: April 03, 2007
If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?

Answer

No. Where a covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the covered entity satisfies the Rule's requirements that it obtain satisfactory assurances from its business associate with the data use agreement. For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.
Are business associates required to restrict their uses and disclosures to the minimum necessary? May a covered entity reasonably rely on a request from a covered entity's business associate as the minimum necessary?

Answer

A covered entity’s contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate’s uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity’s minimum necessary policies and procedures. Given that a business associate contract must limit a business associate’s requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.
Is a physician or other provider considered to be a business associate of a health plan or other payer?

Answer

Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. Each covered entity is acting on its own behalf when a provider submits a claim to a health plan, and when the health plan assesses and pays the claim. However, a business associate relationship could arise if the provider is performing another function on behalf of, or providing services to, the health plan (e.g., case management services) that meet the definition of "business associate" at 45 CFR 160.103.

Last revised: March 26, 2007
Is a health insurance issuer or HMO who provides health
insurance or health coverage to a group health plan a
business associate of the group health plan?

Answer

A health insurance issuer or HMO does not become a business associate simply by
providing health insurance or health coverage to a group health plan. The relationship
between the group health plan and the health insurance issuer or HMO is defined by
the Privacy Rule as an organized health care arrangement (OHCA), with respect to the
individuals they jointly serve or have served. Thus, these covered entities are
permitted to share protected health information that relates to the joint health care
activities of the OHCA. However, where a group health plan contracts with a health
insurance issuer or HMO to perform functions or activities or to provide services that
are in addition to or not directly related to the joint activity of providing insurance, the
health insurance issuer or HMO may be a business associate with respect to those
additional functions, activities, or services.

Last revised: March 26, 2007
Is a reinsurer a business associate of a health plan?

Answer

Generally, no. A reinsurer does not become a business associate of a health plan simply by selling a reinsurance policy to a health plan and paying claims under the reinsurance policy. Each entity is acting on its own behalf when the health plan purchases the reinsurance benefits, and when the health plan submits a claim to a reinsurer and the reinsurer pays the claim. However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.
Is a software vendor a business associate of a covered entity?

Answer

The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity. For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to protected health information. However, when an employee of a contractor, like a software or information technology vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity's workforce, rather than as a business associate. See the definition of "workforce" at 45 CFR 160.103.
How does the HIPAA Privacy Rule change the laws concerning consent for treatment?

Answer

The Privacy Rule relates to uses and disclosures of protected health information, not to whether a patient consents to the health care itself. As such, the Privacy Rule does not affect informed consent for treatment, which is addressed by State law.

Last revised: March 28, 2007
Can a pharmacist use protected health information to fill a prescription that was telephoned in by a patient's physician without the patient's written consent if the patient is a new patient to the pharmacy?

Answer

Yes. The pharmacist is using the protected health information for treatment purposes, and the HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.

Last revised: April 03, 2007
Can health care providers, such as a specialist or hospital, to whom a patient is referred for the first time, use protected health information to set up appointments or schedule surgery or other procedures without the patient's written consent?

Answer

Yes. The HIPAA Privacy Rule does not require covered entities to obtain an individual's consent prior to using or disclosing protected health information about him or her for treatment, payment, or health care operations.
Are health care providers restricted from consulting with other providers about a patient’s condition without the patient’s written authorization?

Answer

No. Consulting with another health care provider about a patient is within the HIPAA Privacy Rule’s definition of “treatment” and, therefore, is permissible. In addition, a health care provider (or other covered entity) is expressly permitted to disclose protected health information about an individual to a health care provider for that provider’s treatment of the individual. See 45 CFR 164.506.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule restrict pharmacists from giving advice about over-the-counter medicines to customers?

Answer

No. A pharmacist may provide advice to customers about over-the-counter medicines. The Privacy Rule permits a covered entity to disclose protected health information about an individual to the individual. See 45 CFR 164.502(a)(1)(i).

Last revised: April 03, 2007
Can a patient have a friend or family member pick up a prescription for her?

Answer

Yes. A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription. See 45 CFR 164.510(b). For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual's care, and the HIPAA Privacy Rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the pharmacist with the names of such persons in advance.
What is the difference between “consent” and “authorization” under the HIPAA Privacy Rule?

Answer

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

By contrast, an “authorization” is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.
May a health care provider disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS)?

Answer

Yes, the HIPAA Privacy Rule permits a provider to disclose protected health information to a health plan for the quality-related health care operations of the health plan, provided that the health plan has or had a relationship with the individual who is the subject of the information, and the protected health information requested pertains to the relationship. See 45 CFR 164.506(c)(4). Thus, a provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, so long as the period for which information is needed overlaps with the period for which the individual is or was enrolled in the health plan.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule permit a covered entity or its collection agency to communicate with parties other than the patient (e.g., spouses or guardians) regarding payment of a bill?

Answer

Yes. The Privacy Rule permits a covered entity, or a business associate acting on behalf of a covered entity (e.g., a collection agency), to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. Therefore, a covered entity, or its business associate, may contact persons other than the individual as necessary to obtain payment for health care services. See 45 CFR 164.506(c) and the definition of “payment” at 45 CFR 164.501. However, the Privacy Rule requires a covered entity, or its business associate, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to restrictions on the use or disclosure of protected health information. See 45 CFR 164.502(b), 164.514(d), and 164.522.
Does the HIPAA Privacy Rule prevent reporting to consumer credit reporting agencies or otherwise create any conflict with the Fair Credit Reporting Act (FCRA)?

Answer

No. The Privacy Rule’s definition of “payment” includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following protected health information about the individual: name and address; date of birth; social security number; payment history; and account number. In addition, disclosure of the name and address of the health care provider or health plan making the report is allowed. The covered entity may perform this payment activity directly, or may carry out this function through a third party, such as a collection agency, under a business associate arrangement.

The Privacy Rule permits uses and disclosures by the covered entity or its business associate as may be required by the Fair Credit Reporting Act (FCRA) or other law. Therefore, the Department does not believe there is a conflict between the Privacy Rule and legal duties imposed on data furnishers by FCRA.
Does the HIPAA Privacy Rule prevent health plans and providers from using debt collection agencies? Does the Privacy Rule conflict with the Fair Debt Collection Practices Act?

Answer

The Privacy Rule permits covered entities to continue to use the services of debt collection agencies. Debt collection is recognized as a payment activity within the "payment" definition. See the definition of "payment" at 45 CFR 164.501. Through a business associate arrangement, the covered entity may engage a debt collection agency to perform this function on its behalf. Disclosures to collection agencies are governed by other provisions of the Privacy Rule, such as the business associate and minimum necessary requirements.

The Department is not aware of any conflict between the Privacy Rule and the Fair Debt Collection Practices Act. Where a use or disclosure of protected health information is necessary for the covered entity to fulfill a legal duty, the Privacy Rule would permit such use or disclosure as required by law.
Are location information services of collection agencies, which are required under the Fair Debt Collection Practices Act, permitted under the HIPAA Privacy Rule?

Answer

"Payment" is broadly defined as activities by health plans or health care providers to obtain premiums or obtain or provide reimbursements for the provision of health care. The activities specified are by way of example and are not intended to be an exclusive listing. Billing, claims management, collection activities and related data processing are expressly included in the definition of "payment." See the definition of "payment" at 45 CFR 164.501. Obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable, and, therefore, would constitute a payment activity. See 45 CFR 164.501. The covered entity and its business associate would also have to comply with any limitations placed on location information services by the Fair Debt Collection Practices Act.
Does the HIPAA Privacy Rule permit an eye doctor to confirm a contact prescription received by a mail-order contact company?

Answer

Yes. The disclosure of protected health information by an eye doctor to a distributor of contact lenses for the purpose of confirming a contact lens prescription is a treatment disclosure, and is permitted under the Privacy Rule at 45 CFR 164.506.

Last revised: April 03, 2007
Does a physician need a patient's written authorization to send a copy of the patient's medical record to a specialist or other health care provider who will treat the patient?

**Answer**

No. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual's authorization, to another health care provider for that provider's treatment of the individual. See 45 CFR 164.506 and the definition of "treatment" at 45 CFR 164.501.
Is a hospital permitted to contact another hospital or health care facility, such as a nursing home, to which a patient will be transferred for continued care, without the patient's authorization?

Answer

Yes. The HIPAA Privacy Rule permits a health care provider to disclose protected health information about an individual, without the individual's authorization, to another health care provider for that provider's treatment or payment purposes, as well as to another covered entity for certain health care operations of that entity. See 45 CFR 164.506 and the definitions of "treatment," "payment," and "health care operations" at 45 CFR 164.501.

Last revised: April 03, 2007
How does the HIPAA Privacy Rule apply to professional liability insurance? Specifically, how can professional liability insurers continue to arrange for and maintain medical liability insurance for health care providers covered by the Rule?

**Answer**

The Privacy Rule permits a covered health care provider to disclose information for "health care operations" purposes, subject to certain requirements. Disclosures by a covered health care provider to a professional liability insurer or a similar entity for the purpose of obtaining or maintaining medical liability coverage or for the purpose of obtaining benefits from such insurance, including the reporting of adverse events, fall within "business management and general administrative activities" under the definition of "health care operations." Therefore, a covered health care provider may disclose individually identifiable health information to a professional liability insurer to the same extent as the provider is able to disclose such information for other health care operations purposes. See 45 CFR 164.502(a)(1)(ii) and the definition of "health care operations" at 45 CFR 164.501.
Does the HIPAA Privacy Rule expand the ability of providers, plans, marketers and others to use my protected health information to market goods and services to me? Does the Privacy Rule make it easier for health care businesses to engage in door-to-door sales and marketing efforts?

Answer

No. The Privacy Rule's limitations on the use or disclosure of protected health information for marketing purposes do not exist in most States today. For example, the Rule requires patients' authorization for the following types of uses or disclosures of protected health information for marketing:

- Selling protected health information to third parties for their use and re-use. Thus, under the Rule, a hospital or other provider may not sell names of pregnant women to baby formula manufacturers or magazines without an authorization.

- Disclosing protected health information to outsiders for the outsiders' independent marketing use. Under the Rule, doctors may not provide patient lists to pharmaceutical companies for those companies' drug promotions without an authorization.

Without these Privacy Rule restrictions, these activities could occur with no authorization from the individual in most jurisdictions. In addition, if a State law provided additional limitations on disclosures of information for related activities, the Privacy Rule generally would not interfere with those laws.

Moreover, under the "business associate" provisions of the Privacy Rule, a covered entity may not give protected health information to a telemarketer, door-to-door salesperson, or other third party it has hired to make permitted communications (for example, about a covered entities' own goods and services) unless that third party has agreed by contract to use the information only for communicating on behalf of the covered entity. Without the Privacy Rule, there may be no restrictions on how third parties re-use information they obtain from health plans and providers. See the fact sheet and frequently asked questions on this web site about the business associate standard for more information.

Last revised: April 03, 2007
Can contractors (business associates) use protected health information for its own marketing purposes?

Answer

No. While covered entities may share protected health information with their contractors who meet the definition of “business associates” under the HIPAA Privacy Rule, that definition is limited to contractors that obtain protected health information to perform or assist in the performance of certain health care operations on behalf of covered entities. Thus, business associates, with limited exceptions, cannot use protected health information for their own purposes. Although, under the HIPAA statute, the Privacy Rule cannot govern contractors directly, the Rule does set clear parameters for how covered entities may contract with business associates. See 45 CFR 164.502(e) and 164.504(e), and the definition of “business associate” at 45 CFR 160.103.

Further, the Privacy Rule expressly prohibits health plans and covered health care providers from selling protected health information to third parties for the third party’s own marketing activities, without authorization. So, for example, a pharmacist cannot, without patient authorization, sell a list of patients to a pharmaceutical company, for the pharmaceutical company to market its own products to the individuals on the list.
Can telemarketers obtain my health information and use it to call me to sell good and services?

Answer

Under the HIPAA Privacy Rule, a covered entity can share protected health information with a telemarketer only if the covered entity has either obtained the individual’s prior written authorization to do so, or has entered into a business associate relationship with the telemarketer for the purpose of making a communication that is not marketing, such as to inform individuals about the covered entity’s own goods or services.

If the telemarketer is a business associate under the Privacy Rule, it must agree by contract to use the information only for communicating on behalf of the covered entity, and not to market its own goods or services (or those of another third party).
Will the HIPAA Privacy Rule hinder medical research by making doctors and others less willing and/or able to share with researchers information about individual patients?

Answer

We do not believe that the Privacy Rule will hinder medical research. Indeed, patients and health plan members should be more willing to authorize disclosures of their information for research and to participate in research when they know their information is protected. For example, in genetic studies conducted at the National Institutes of Health, nearly 32 percent of eligible people offered a test for breast cancer risk declined to take it. The overwhelming majority of those who refuse cite concerns about health insurance discrimination and loss of privacy as the reason. The Privacy Rule both permits important research and, at the same time, encourages patients to participate in research by providing much needed assurances about the privacy of their health information.

The Privacy Rule will require some covered health care providers and health plans to change their current practices related to documenting research uses and disclosures. It is possible that some covered health care providers and health plans may conclude that the Rule’s requirements for research uses and disclosures are too burdensome and will choose to limit researchers’ access to protected health information. We believe few providers will take this route, however, because the Common Rule includes similar, and more rigorous requirements, that have not impaired the willingness of researchers to undertake Federally-funded research. For example, unlike the Privacy Rule, the Common Rule requires an Institutional Review Board (IRB) review for all research proposals under its purview, even if informed consent is to be sought. The Privacy Rule requires documentation of IRB or Privacy Board approval only if patient authorization for the use or disclosure of protected health information for research purposes is to be altered or waived. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.
When is an authorization required from the patient before a provider or health plan engages in marketing to that individual?

Answer

The HIPAA Privacy Rule expressly requires an authorization for uses or disclosures of protected health information for all marketing communications, except in two circumstances: (1) when the communication occurs in a face-to-face encounter between the covered entity and the individual; or (2) the communication involves a promotional gift of nominal value.

If the marketing communication involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.

Last revised: March 26, 2007
How can I distinguish between activities for treatment or health care operations versus marketing activities?

Answer

The overlap among common usages of the terms "treatment," "healthcare operations," and "marketing" is unavoidable. For instance, in recommending treatments, providers and health plans sometimes advise patients to purchase goods and services. Similarly, when a health plan explains to its members the benefits it provides, it too is encouraging the use or purchase of goods and services.

The HIPAA Privacy Rule defines these terms specifically, so they can be distinguished. For example, the Privacy Rule excludes treatment communications and certain health care operations activities from the definition of "marketing." If a communication falls under one of the definition's exceptions, the marketing rules do not apply. In these cases, covered entities may engage in the activity without first obtaining an authorization. See the fact sheet on this web site about marketing, as well as the definition of "marketing" at 45 CFR 164.501, for more information.

However, if a health care operation communication does not fall within one of these specific exceptions to the marketing definition, and the communication falls under the definition of "marketing," the Privacy Rule's provisions restricting the use or disclosure of protected health information for marketing purposes will apply. For these marketing communications, the individual's authorization is required before a covered entity may use or disclose protected health information.
Do disease management, health promotion, preventive care, and wellness programs fall under the HIPAA Privacy Rule's definition of "marketing"?

Answer

Generally, no. To the extent the disease management or wellness program is operated by the covered entity directly or by a business associate, communications about such programs are not marketing because they are about the covered entity’s own health-related services. So, for example, a hospital’s Wellness Department could start a weight-loss program and send a flyer to all patients seen in the hospital over the past year who meet the definition of obese, even if those individuals were not specifically seen for obesity when they were in the hospital.

Moreover, a communication that merely promotes health in a general manner and does not promote a specific product or service from a particular provider does not meet the definition of “marketing.” Such communications may include population-based activities in the areas of health education or disease prevention. Examples of general health promotional material include mailings reminding women to get an annual mammogram; mailings providing information about how to lower cholesterol, new developments in health care (e.g., new diagnostic tools), support groups, organ donation, cancer prevention, and health fairs.
Is it marketing for a covered entity to describe products or services that are provided by the covered entity to its patients, or to describe products or services that are included in the health plan’s plan of benefits of the health plan?

Answer

No. The HIPAA Privacy Rule excludes from the definition of "marketing" communications made to describe a covered entity’s health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication. Thus, it would not be marketing for a physician who has developed a new anti-snore device to send a flyer describing it to all of her patients (whether or not each patient has actually sought treatment for snoring). Nor would it be marketing for an ophthalmologist or health plan to send existing patients or members discounts for eye-exams or eye-glasses available only to the patients and members. Similarly, it would not be marketing for an insurance plan to send its members a description of covered benefits, payment schedules, and claims procedures.
Is it marketing for a covered entity to describe the entities participating in a health care provider network or a health plan network?

Answer:

No. The HIPAA Privacy Rule excludes from the definition of "marketing," communications by a covered entity to describe the entities participating in a health care provider network or a health plan network. Thus, it would not be marketing for a health plan or insurer to mail its members or enrollees a list of health care providers in the health plan network or for an independent physicians association to send its patients a preferred provider list.
Is it marketing for an insurance plan or health plan to send enrollees notices about changes, replacements, or improvements to existing plans?

Answer

No. The HIPAA Privacy Rule excludes from the definition of "marketing," communications about replacements of, or enhancements to, a health plan. Therefore, notices about changes in deductibles, co-pays and types of coverage, such as prescription drugs, are not marketing. Likewise, a notice to a family warning that a student reaching the age of majority on a parental policy will lose coverage, then offering continuation coverage, would not be considered marketing. Nor are special health care policies such as guaranteed issue products and conversion policies considered marketing. Similarly, notices from a health plan about its long term care benefits would not be considered marketing.

It would be considered marketing, however, for a health plan to send to its members promotional material about insurance products that are considered to be "excepted benefits" (described in section 2791(c)(1) of the Public Health Service Act), such as accident only policies. It would likewise be marketing for health plans to describe other lines of insurance, such as life insurance policies. Generally, such communications require authorizations.

Last revised: April 03, 2007
Can health plans communicate about health-related products or services to enrollees that add value to, but are not part of, a plan of benefits?

Answer

Yes. The provision of value-added items or services (VAIS) is a common practice, particularly for managed care organizations. Under the HIPAA Privacy Rule, communications may qualify under the marketing exception for a communication about a health plan's plan of benefits, even if the VAIS are not considered plan benefits for the Adjusted Community Rate purposes. To qualify for this exclusion, however, the VAIS must meet two conditions. First, they must be health-related. Therefore, discounts offered by Medicare + Choice or other managed care organizations for eyeglasses may be considered part of the plan's benefits, whereas discounts to attend movie theaters will not. Second, such items and services must demonstrably "add value" to the plan's membership and not merely be a pass-through of a discount or item available to the public at large.

So, a Medicare + Choice or other managed care organization could offer its members a special discount opportunity for eyeglasses and contact lenses without obtaining authorizations if the discount were only available through membership in the managed care organization. However, such communications would need an authorization if the members would be able to obtain such discounts directly from the eyeglass store.

Similarly, a Medicare + Choice or other managed care organization could offer its members a special discount opportunity for a prescription drug card benefit or for a health/fitness club membership, which is not available to consumers on the open market. On the other hand, a Medicare+Choice or other managed care organization would need an authorization to notify its members of a discount to a movie theater available only to its members.

Last revised: April 03, 2007
Can a doctor or pharmacy be paid to make a prescription refill reminder without a prior authorization under the HIPAA Privacy Rule?

Answer

Yes. It is not marketing for a doctor to make a prescription refill reminder even if a third party pays for the communication. The prescription refill reminder is considered treatment. The communication is therefore excluded from the definition of marketing and does not require a prior authorization. Similarly, it is not marketing when a doctor or pharmacy is paid by a pharmaceutical company to recommend an alternative medication to patients. Communications about alternative treatments are excluded from the definition of marketing and do not require a prior authorization. The simple receipt of remuneration does not transform a treatment communication into a commercial promotion of a product or service.

Furthermore, covered entities may use a legitimate business associate to assist them in making such permissible communications. For instance, if a pharmacist that has been paid by a third party contracts with a mail house to send out prescription refill reminders to the pharmacist's patients, neither the mail house nor the pharmacist needs a prior authorization. However, a covered entity would require an authorization if it sold protected health information to a third party for the third party's marketing purposes.
Are appointment reminders allowed under the HIPAA Privacy Rule without authorizations?

Answer

Yes, appointment reminders are considered part of treatment of an individual and, therefore, can be made without an authorization.

Last revised: April 03, 2007
What are examples of "alternative treatments" that are excepted from the HIPAA Privacy Rule's definition of "marketing"?

Answer

Alternative treatments are treatments that are within the range of treatment options available to an individual. For example, it would be an alternative treatment communication if a doctor, in response to an inquiry from a patient with skin rash about the range of treatment options, mails the patient a letter recommending that the patient purchase various ointments and medications described in brochures enclosed with the letter. Alternative treatment could also include alternative medicine. Thus, alternative treatments would include communications by a nurse midwife who recommends or sells vitamins and herbal preparations, dietary and exercise programs, massage services, music or other alternative types of therapy to her pregnant patients.
Are prior authorizations required when a doctor or health plan distributes promotional gifts of nominal value?

Answer

No. In a specific exception, the HIPAA Privacy Rule allows covered entities to distribute items commonly known as promotional gifts of nominal value without prior authorization, even if such items are distributed with the intent of encouraging the receiver to buy the products or services. This authorization exception generally applies to items and services of a third party, whether or not they are health-related, or items and services of the covered entity that are not health-related. A covered doctor, for instance, may send patients items such as pens, note-pads, and cups embossed with a health plan's logo without prior authorization. Similarly, dentists may give patients free toothbrushes, floss and toothpaste.
Are health care providers required to seek a prior authorization before discussing a product or service with a patient, or giving a product or service to a patient, in a face-to-face encounter?

Answer:

No. In face-to-face encounters, the HIPAA Privacy Rule allows covered entities to give or discuss products or services, even when not health-related, to patients without a prior authorization. This exception prevents unnecessary intrusion into the doctor-patient relationship.

Physicians may give out free pharmaceutical samples, regardless of their value. Similarly, hospitals may give infant supplies to new mothers. Moreover, the face-to-face exception would allow providers to leave general circulation materials in their offices for patients to pick up during office visits.
Must insurance agents that are business associates of a health plan seek a prior authorization before talking to a customer in a face-to-face encounter about the insurance company's other lines of business?

Answer

No. In the specific case of face-to-face encounters, the HIPAA Privacy Rule allows health plans and their business associates to market both health and non-health insurance products to individuals.

Last revised: March 26, 2007
May covered entities use information regarding specific clinical conditions of individuals in order to communicate about products or services for such conditions without a prior authorization?

Answer

Yes, if the communication is for the individual's treatment or for case management, care coordination, or the recommendation of alternative therapies. The HIPAA Privacy Rule permits the use of clinical information to the extent it is reasonably necessary for these communications. Similarly, population-based activities in the areas of health education or disease prevention are not considered marketing when they promote health in a general manner. Again clinical information may be used for such communications, such as in targeting a public education campaign.

Last revised: March 26, 2007
Are communications concerning information to beneficiaries about government programs or government-sponsored programs "marketing" under the HIPAA Privacy Rule?

Answer

No. Communications about government and government-sponsored programs do not fall within the definition of "marketing." There is no commercial component to communications about benefits available through public programs. Therefore, a covered entity is permitted to use and disclose protected health information to communicate about eligibility for such programs as Medicare, Medicaid, or the State Children's Health Insurance Program (SCHIP).

Last revised: April 03, 2007
Must a health care provider or other covered entity obtain permission from a patient prior to notifying public health authorities of the occurrence of a reportable disease?

Answer

No. All States have laws that require providers to report cases of specific diseases to public health officials. The HIPAA Privacy Rule permits disclosures that are required by law. Furthermore, disclosures to public health authorities that are authorized by law to collect or receive information for public health purposes are also permissible under the Privacy Rule. In order to do their job of protecting the health of the public, it is frequently necessary for public health officials to obtain information about the persons affected by a disease. In some cases they may need to contact those affected in order to determine the cause of the disease to allow for actions to prevent further illness.

The Privacy Rule continues to allow for the existing practice of sharing protected health information with public health authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting deaths and births, investigating the occurrence and cause of injury and disease, and monitoring adverse outcomes related to food (including dietary supplements), drugs, biological products, and medical devices. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Last revised: April 03, 2007
Does the public health provision of the HIPAA Privacy Rule require covered entities to make public health disclosures?

Answer

No. The Privacy Rule's public health provision permits, but does not require, covered entities to make such disclosures. This provision is intended to allow covered entities to continue current voluntary reporting practices that are critically important to public health and safety. The Rule also permits covered entities to disclose protected health information when State or other law requires covered entities to make disclosures for public health purposes. For instance, many State laws require health care providers to report certain diseases, cases of child abuse, births, or deaths, and the Privacy Rule permits covered entities to disclose protected health information, without authorization, to make such reports. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Last revised: April 03, 2007
May covered entities disclose facially identifiable protected health information, such as name, address, and social security number, for public health purposes?

Answer

Yes. The HIPAA Privacy Rule permits covered entities to disclose the amount and type of protected health information that is needed for public health purposes. In some cases, the disclosure will be required by other law, in which case, covered entities may make the required disclosure pursuant to 45 CFR 164.512(a) of the Rule. For disclosures that are not required by law, covered entities may disclose, without authorization, the information that is reasonably limited to that which is minimally necessary to accomplish the intended purpose of the disclosure. For routine or recurring public health disclosures, a covered entity may develop protocols as part of its minimum necessary policies and procedures to address the type and amount of information that may be disclosed for such purposes. Covered entities may also rely on the requesting public health authority’s determination of the minimally necessary information. See the fact sheet and frequently asked questions on this web site about the public health and minimum necessary standards for more information.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule's public health provision permit covered entities to disclose protected health information to authorities such as the National Institutes of Health (NIH)?

Answer

The definition of a “public health authority” requires that an agency’s official mandate include the responsibility for public health matters. The mandate can be responsibility for public health matters, generally, or it can be for specific public health programs. Furthermore, an agency’s official mandate does not have to be exclusively or primarily for public health. Therefore, to the extent a government agency has public health matters as part of its official mandate, it qualifies as a public health authority. For instance, various Department of Health and Human Service agencies, such as NIH and the Health Resources and Services Administration (HRSA), are authorized by law to assist the Secretary of Health and Human Services in carrying out the purposes of section 301 of the Public Health Service Act. Those agencies are public health authorities under the Rule, even if they have other non-public health mandates. To the extent a public health authority is authorized by law to collect or receive information for the public health purposes specified in the public health provision, covered entities may disclose protected health information to such public health authorities without authorization pursuant to the public health provision. See the fact sheet and frequently asked questions on this web site about the public health provision for more information.

Last revised: March 26, 2007
To whom may covered entities make public health disclosures regarding a product regulated by the Food and Drug Administration (FDA) when more than one person is identified on the product label?

Answer

Covered entities may identify persons responsible for an FDA-regulated product by using the product label, the literature that accompanies the product, or other sources of labeling, such as the Physician's Desk Reference. If multiple persons are named, covered entities may choose any of the persons named by these sources. See the fact sheet and frequently asked questions on this website about the public health provision for more information.

Last revised: May 31, 2007
Is a covered entity permitted to disclose protected health information under the HIPAA Privacy Rule's public health provision when the link between an adverse event and a product regulated by the Food and Drug Administration (FDA) is only suspected?

Answer

Yes. In most instances when a covered entity makes an adverse event report to a person responsible for an FDA-regulated product, the covered entity will suspect, but not know, the product is the cause of the event. Determining whether the product is related to the adverse event almost always requires follow up with the covered entity which in turn may need further contact with the patient. FDA and product manufacturers receive a great deal of important information about the safety of regulated products from these reports. To limit such reports to those instances where the covered entity is convinced of the link between the product and the event would reduce the amount of useful safety, quality and effectiveness data available to the agency as well as to product manufacturers. This would limit significantly FDA’s ability to protect the public health by helping to assure that only safe and effective products are marketed in the U.S. Accordingly, covered entities may disclose the minimum amount of protected health information that is reasonably necessary to report suspected adverse events associated with an FDA-regulated product. See the fact sheet and frequently asked questions on this web site about the public health and minimum necessary standards for more information.

Last revised: May 31, 2007
Does the HIPAA Privacy Rule's public health provision permit covered entities to disclose protected health information without authorization to a manufacturer of a product regulated by the Food and Drug Administration (FDA) for use by the manufacturer to assess the effectiveness of its marketing campaign?

Answer

No. The public health provision is intended to facilitate the flow of information that is essential to the FDA's public health mission. The provision does not permit covered entities to disclose protected health information to a manufacturer for the manufacturer's commercial purposes, or for any other non-public health purpose. For example, the Rule does not permit a covered entity to provide a drug manufacturer with a list of persons who prefer a different flavored cough syrup over the flavor of the manufacturer's product. Rather, this provision permits covered entities to disclose protected health information as necessary to continue current voluntary reporting of adverse events and similar reports that are necessary to ensure the quality, safety, or effectiveness of an FDA-regulated product. For instance, a covered entity would be permitted to report a concern to a drug manufacturer that its cough syrup might be unsafe based on the belief that a difference in the taste could be due to drug tampering or a manufacturing problem. Likewise, a covered health care provider would be permitted to disclose protected health information to a drug manufacturer to report that the failure of a patient's medical condition to improve may be due to the drug's ineffectiveness. In making such a report, the covered entity may disclose the protected health information that is reasonably necessary to achieve the purpose of the report. See the fact sheet and frequently asked questions on this website about the public health and minimum necessary standards for more information.
Does the HIPAA Privacy Rule's public health provision permit covered health care providers to disclose protected health information concerning the findings of pre-employment physicals, drug tests, or fitness-for-duty examinations to an individual's employer?

Answer

The public health provision permits covered health care providers to disclose an individual's protected health information to the individual's employer without authorization in very limited circumstances. First, the covered health care provider must provide the health care service to the individual at the request of the individual's employer or as a member of the employer's workforce. Second, the health care service provided must relate to the medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury. Third, the employer must have a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on or act on such information. For example, OSHA requires employers to monitor employees' exposures to certain substances and to take specific actions when an employee's exposure level exceeds a specified limit. A covered entity which tests an individual for such an exposure level at the request of the individual's employer may disclose that test result to the employer without authorization.

Generally, pre-placement physicals, drug tests, and fitness-for-duty examinations are not performed for such purposes. However, to the extent such an examination is conducted at the request of the employer for the purpose of such workplace medical surveillance or work-related illness or injury, and the employer needs the information to comply with the requirements of OSHA, MSHA, or similar State law, the protected health information the employer needs to meet such legal obligation may be discussed to the employer without authorization. Covered health care providers who make such disclosures must provide the individual with written notice that the information is to be disclosed to his or her employer (or by posting the notice at the worksite if the service is provided there). When a health care service does not meet the above requirements, covered entities may not disclose an individual's protected health information to the individual's employer without an authorization, unless the disclosure is otherwise permitted without authorization by other provisions of the Rule. However, nothing in the Rule prohibits an employer from conditioning employment on an individual providing an authorization for the disclosure of such information.
Are some of the criteria so subjective that inconsistent determinations may be made by Institutional Review Boards (IRB) and Privacy Boards reviewing similar or identical research projects?

Answer

Under the HIPAA Privacy Rule, IRBs and Privacy Boards need to use their judgment as to whether the waiver criteria have been satisfied. Several of the waiver criteria are closely modeled on the Common Rule’s criteria for the waiver of informed consent and for the approval of a research study. Thus, it is anticipated that IRBs already have experience in making the necessarily subjective assessments of risks. While IRBs or Privacy Boards may reach different determinations, the assessment of the waiver criteria through this deliberative process is a crucial element in the current system of safeguarding research participants’ privacy. The entire system of local IRBs is, in fact, predicated on a deliberative process that permits local IRB autonomy. The Privacy Rule builds upon this principle; it does not change it. Nonetheless, the Department will consider issuing guidance as necessary and appropriate to address concerns that may arise during implementation of these provisions. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.

Last revised: March 26, 2007
Does the HIPAA Privacy Rule prohibit researchers from conditioning participation in a clinical trial on an authorization to use/disclose existing protected health information?

Answer

No. The Privacy Rule does not address conditions for enrollment in a research study. Therefore, the Privacy Rule in no way prohibits researchers from conditioning enrollment in a research study on the execution of an authorization for the use of pre-existing health information.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule permit the creation of a database for research purposes through an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization?

Answer

Yes. A covered entity may use or disclose protected health information without individuals' authorizations for the creation of a research database, provided the covered entity obtains documentation that an IRB or Privacy Board has determined that the specified waiver criteria were satisfied. Protected health information maintained by a covered entity in such a research database could be used or disclosed for future research studies as permitted by the Privacy Rule – that is, for future studies in which individual authorization has been obtained or where the Rule would permit research without an authorization, such as pursuant to an IRB or Privacy Board waiver. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Last revised: April 03, 2007
Can researchers continue to access existing databanks or repositories that are maintained by covered entities, even if those databases were created prior to the compliance date without patient permission or without a waiver of informed consent by an Institutional Review Board (IRB)?

Answer

Yes. Under the HIPAA Privacy Rule, covered entities may use or disclose protected health information from existing databases or repositories for research purposes either with individual authorization as required at 45 CFR 164.508, or with a waiver of individual authorization as permitted at 45 CFR 164.512(i). See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review Boards.
How does the Rule help Institutional Review Boards (IRB) handle the additional responsibilities imposed by the HIPAA Privacy Rule?

Answer

Recognizing that some institutions may not have IRBs, or that some IRBs may not have the expertise needed to review research that requires consideration of risks to privacy, the Privacy Rule permits the covered entity to accept documentation of waiver of authorization from an alternative body called a Privacy Board—which could have fewer members, and members with different expertise than IRBs. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

In addition, the Rule allows an IRB to use expedited review procedures as permitted by the Common Rule to review and approve requests for waiver of authorizations. Similarly, the Rule permits Privacy Boards to use an expedited review process when the research involves no more than a minimal privacy risk to the individuals. An expedited review process permits covered entities to accept documentation of waiver of authorization when only one or more members of the IRB or Privacy Board have conducted the review. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule.
By establishing new waiver criteria and authorization requirements, hasn't the HIPAA Privacy Rule, in effect, modified the Common Rule?

Answer

No. Where both the Privacy Rule and the Common Rule apply, both regulations must be followed. The Privacy Rule regulates only the content and conditions of the documentation that covered entities must obtain before using or disclosing protected health information for research purposes. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule.

Last revised: May 31, 2007
Is documentation of Institutional Review Boards (IRB) and Privacy Board approval required by the HIPAA Privacy Rule before a covered entity would be permitted to disclose protected health information for research purposes without an individual's authorization?

Answer

No. The HIPAA Privacy Rule requires documentation of waiver approval by either an IRB or a Privacy Board, not both. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule require a covered entity to create an Institutional Review Board (IRB) or Privacy Board before using or disclosing protected health information for research?

Answer

No. The IRB or Privacy Board could be created by the covered entity or the recipient researcher, or it could be an independent board. See the fact sheets and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Last revised: April 03, 2007
What does the HIPAA Privacy Rule say about a research participant's right of access to research records or results?

Answer

With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about themselves that is maintained by a covered entity or its business associate in a "designated record set." A designated record set is basically a group of records which a covered entity uses to make decisions about individuals, and includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. While it may be unlikely that a researcher would be maintaining a designated record set, any research records or results that are actually maintained by the covered entity as part of a designated record set would be accessible to research participants unless one of the Privacy Rule's permitted exceptions applies.

One of the permitted exceptions applies to protected health information created or obtained by a covered health care provider/researcher for a clinical trial. The Privacy Rule permits the individual's access rights in these cases to be suspended while the clinical trial is in progress, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial. In addition, the health care provider/researcher must inform the research participant that the right to access protected health information will be reinstated at the conclusion of the clinical trial.
Do the HIPAA Privacy Rule's requirements for authorization and the Common Rule's requirements for informed consent differ?

Answer

Yes. Under the Privacy Rule, a patient's authorization is for the use and disclosure of protected health information for research purposes. In contrast, an individual's informed consent, as required by the Common Rule and the Food and Drug Administration's (FDA) human subjects regulations, is a consent to participate in the research study as a whole, not simply a consent for the research use or disclosure of protected health information. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule. For this reason, there are important differences between the Privacy Rule's requirements for individual authorization, and the Common Rule's and FDA's requirements for informed consent. However, the Privacy Rule's authorization elements are compatible with the Common Rule's informed consent elements. Thus, both sets of requirements can be met by use of a single, combined form, which is permitted by the Privacy Rule. For example, the Privacy Rule allows the research authorization to state that the authorization will be valid until the conclusion of the research study, or to state that the authorization will not have an expiration date or event. This is compatible with the Common Rule's requirement for an explanation of the expected duration of the research subject's participation in the study. It should be noted that where the Privacy Rule, the Common Rule, and/or FDA's human subjects regulations are applicable, each of the applicable regulations will need to be followed.
When is a researcher a covered health care provider under HIPAA?

Answer

A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See 45 CFR 160.102, 160.103. For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf. For further assistance in determining covered entity status, see the “decision tool” at www.hhs.gov/ocr/hipaa/.

Last revised: March 26, 2007
When does a covered entity have discretion to determine whether a research component of the entity is part of their covered functions, and therefore, subject to the HIPAA Privacy Rule?

Answer

A covered entity that qualifies as a hybrid entity, meaning that the entity is a single legal entity that performs both covered and non-covered functions, may choose whether it wants to be a hybrid entity. If such a covered entity decides not to be a hybrid entity then it, and all of its components, are subject to the Privacy Rule in its entirety. Therefore, if a researcher is an employee or workforce member of a covered entity that has decided not to be a hybrid entity, the researcher is part of the covered entity and is, therefore, subject to the Privacy Rule.

If a covered entity decides to be a hybrid entity, it must define and designate its health care component(s). Research components of a hybrid entity that function as health care providers and engage in standard electronic transactions must be included in the hybrid entity’s health care component(s), and be subject to the Privacy Rule.

However, research components that function as health care providers, but do not engage in standard electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, a hybrid entity, such as a university, has the option to include or exclude a research laboratory, that functions as a health care provider but does not engage in electronic transactions, as part of the hybrid entity’s health care component. If such a research laboratory is included in the hybrid entity’s health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity’s health care component, the employees or workforce members of the laboratory are not subject to the Privacy Rule.
If a research subject revokes his or her authorization to have protected health information used or disclosed for research, does the HIPAA Privacy Rule permit a researcher/covered health care provider to continue using the protected health information already obtained prior to the time the individual revoked his or her authorization?

Answer

Covered entities may continue to use and disclose protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. An individual may not revoke an authorization to the extent the covered entity has acted in reliance on the authorization. For research uses and disclosures, this reliance exception at 45 CFR 164.508(b)(5)(i) permits the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study. For example, the reliance exception would permit the continued use and disclosure of protected health information to account for a subject’s withdrawal from the research study, as necessary to incorporate the information as part of a marketing application submitted to the Food and Drug Administration, to conduct investigations of scientific misconduct, or to report adverse events.

However, the reliance exception would not permit a covered entity to continue disclosing additional protected health information to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her authorization.

Last revised: May 31, 2007
Can the preparatory research provision of the HIPAA Privacy Rule at 45 CFR 164.512(i)(1)(ii) be used to recruit individuals into a research study?

Answer

The preparatory research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity’s site. As such, a researcher who is an employee or a member of the covered entity’s workforce could use protected health information to contact prospective research subjects. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information. See 45 CFR 164.502(a)(1)(i). Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards. However, a researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board as permitted at 45 CFR 164.512(i)(1)(i). The IRB or Privacy Board waiver of authorization permits the partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information as necessary for the researcher to be able to contact and recruit individuals into the study.
Does the HIPAA Privacy Rule require documentation of Institutional Review Board (IRB) or Privacy Board approval of an alteration or waiver of individual authorization before a covered entity may use or disclose protected health information for any of the following provisions: (1) for preparatory research at 45 CFR 164.512(i)(1)(ii), (2) for research on the protected health information of decedents at 45 CFR 164.512(i)(1)(iii), or (3) a limited data set with a data use agreement as stipulated at 45 CFR 164.51

Answer

No. Documentation of IRB or Privacy Board approval of an alteration or waiver of individual authorization is only needed before a covered entity may use or disclose protected health information under 45 CFR 164.512(i)(1)(i) (PDF - 61KB). See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Download Acrobat Reader to view and print PDF files.

Last revised: June 21, 2007
If research subjects' consent was obtained before the compliance date, but the Institutional Review Board (IRB) subsequently modifies the informed consent document after the compliance date and requires that subjects be reconsented, is authorization now required from these previously enrolled research subjects under the HIPAA Privacy Rule?

**Answer**

Yes. If informed consent or reconsent (i.e., asked to sign a revised consent or another informed consent) is obtained from research subjects after the compliance date, the covered entity must obtain individual authorization as required at 45 CFR 164.508 for the use or disclosure of protected health information once the consent obtained before the compliance date is no longer valid for the research. The revised informed consent document may be combined with the authorization elements required by 45 CFR 164.508. See the fact sheet and frequently asked questions about the research provisions on this website for more information about Institutional Review Boards.
Can covered entities continue to disclose adverse event reports that contain protected health information to the Department of Health and Human Services (HHS) Office for Human Research Protections?

Answer

Yes. The Office for Human Research Protections is a public health authority under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to report adverse events to the Office for Human Research Protections either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for public health activities as permitted at 45 CFR 164.512(b).

Last revised: April 03, 2007
Can covered entities continue to disclose protected health information to the HHS Office for Human Research Protections for purposes of determining compliance with the HHS regulations for the protection of human subjects (45 CFR Part 46)?

Answer

Yes. The Office for Human Research Protections is a health oversight agency under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to the Office for Human Research Protections for such compliance investigations either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for health oversight activities as permitted at 45 CFR 164.512(d).

Last revised: April 03, 2007
Won't the HIPAA Privacy Rule's minimum necessary standard impede the ability of workers' compensation insurers, State administrative agencies, and employers to obtain the health information needed to pay injured or ill workers the benefits guaranteed them under State workers' compensation system?

Answer

No. The Privacy Rule is not intended to impede the flow of health information to those who need it to process or adjudicate claims, or coordinate care, for injured or ill workers under workers' compensation systems. The minimum necessary standard generally requires covered entities to make reasonable efforts to limit uses and disclosures of, as well as requests for, protected health information to the minimum necessary to accomplish the intended purpose. For disclosures of protected health information made for workers' compensation purposes under 45 CFR 164.512(l), the minimum necessary standard permits covered entities to disclose information to the full extent authorized by State or other law. In addition, where protected health information is requested by a State workers' compensation or other public official for such purposes, covered entities are permitted reasonably to rely on the official's representations that the information requested is the minimum necessary for the intended purpose. See 45 CFR 164.514(d)(3)(iii)(A).

For disclosures of protected health information for payment purposes, covered entities may disclose the type and amount of information necessary to receive payment for any health care provided to an injured or ill worker.

The minimum necessary standard does not apply to disclosures that are required by State or other law or made pursuant to the individual's authorization.
Does an individual have a right under the HIPAA Privacy Rule to restrict the protected health information his or her health care provider discloses for workers' compensation purposes?

Answer

Individuals do not have a right under the Privacy Rule at 45 CFR 164.522(a) to request that a covered entity restrict a disclosure of protected health information about them for workers' compensation purposes when that disclosure is required by law or authorized by, and necessary to comply with, a workers' compensation or similar law. See 45 CFR 164.522(a) and 164.512(a) and (l).

Last revised: March 26, 2007
Does the HIPAA Privacy Rule permit a health care provider to disclose an injured or ill worker's protected health information without his or her authorization when requested for purposes of adjudicating the individual's workers' compensation claim?

Answer

Covered entities are permitted to disclose protected health information for such purposes as authorized by, and to the extent necessary to comply with, workers' compensation law. See 45 CFR 164.512(l). In addition, the Privacy Rule generally permits covered entities to disclose protected health information in the course of any judicial or administrative proceeding in response to a court order, subpoena, or other lawful process. See 45 CFR 164.512(e).

Last revised: March 26, 2007
I am a health care provider and my State law says I have to provide a workers' compensation insurer, upon request, with an injured workers' records that related to treatment or hospitalization for which compensation is being sought. Am I permitted to disclose the information required by my State law?

Answer:

Yes. The HIPAA Privacy Rule permits a covered entity to disclose protected health information as necessary to comply with State law. No minimum necessary determination is required. See 45 CFR 164.512(a) and 164.502(b) (PDF - 3 pages).
My State law says I may disclose records, relating to the treatment I provided to an injured worker, to a workers' compensation insurer for purposes of determining the amount of or entitlement to payment under the workers' compensation system. Am I allowed to share this information under the HIPAA Privacy Rule?

Answer

Yes. A covered entity is permitted to disclose an individual's protected health information as necessary to comply with and to the full extent authorized by workers' compensation law. See 45 CFR 164.512(l).
My State law says I may provide information regarding an injured workers' previous condition, which is not directly related to the claim for compensation, to an employer or insurer if I obtain the workers' written release. Am I permitted to make this disclosure under the HIPAA Privacy Rule?

Answer

A covered entity may disclose protected health information where the individual's written authorization has been obtained, consistent with the Privacy Rule's requirements at 45 CFR 164.508. Thus, a covered entity would be permitted to make the above disclosure if the individual signed such an authorization.
Are hospitals or other health care providers required to provide their notices to patients they treat in an emergency?

Answer

Hospitals and other covered health care providers with a direct treatment relationship with individuals are not required to provide their notices to patients at the time they are providing emergency treatment. In these situations, the HIPAA Privacy Rule requires only that providers give patients a notice when it is practical to do so after the emergency situation has ended. In addition, where notice is delayed by an emergency treatment situation, the Privacy Rule does not require that providers make a good faith effort to obtain the patient's written acknowledgment of receipt of the notice.

Last revised: March 26, 2007
If a health care provider chooses to obtain an individual's consent to use or disclose protected health information about them, does the provider also have to make a good faith effort to obtain the individual's acknowledgement of the notice?

Answer

Yes. The HIPAA Privacy Rule requires that a covered health care provider with a direct treatment relationship with individuals make a good faith effort to obtain written acknowledgments from those individuals that they have received the provider's notice, regardless of whether the provider also chooses to obtain the individuals' consent. However, those providers that choose to obtain consent from individuals have discretion to design one form that includes both a consent and the acknowledgment of receipt of the notice.
Can covered entities distribute their notices as part of other mailings or distributions?

Answer

Yes. The HIPAA Privacy Rule provides covered entities with discretion in this area; no special or separate mailings or distributions are required to satisfy the Privacy Rule's notice distribution requirements. Thus, a health plan distributing its notice through the mail, in accordance with 45 CFR 164.520(c)(1), may do so as part of another mailing to the individual (e.g., by including the notice with Summary Plan Descriptions). Similarly, a covered entity that e-mails its notice to an individual, in accordance with 45 CFR 164.520(c)(3), may include additional materials in the e-mail. No separate e-mail is required. However, the Privacy Rule continues to prohibit covered entities from combining the notice in a single document with an authorization form (see 45 CFR 164.508(b)(3)); and direct treatment providers, other than in emergency situations, must provide the notice at or before the date of first service delivery, and must make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice.
Does the HIPAA Privacy Rule require a health care provider to obtain a new acknowledgement of receipt of the notice from patients if the facility changes its privacy policy?

Answer

No. A covered health care provider with a direct treatment relationship with individuals is required to make a good faith effort to obtain an individual's acknowledgement of receipt of the notice only at the time the provider first gives the notice to the individual -- that is, at first service delivery. See 45 CFR 164.520(c)(2).

Last revised: April 03, 2007
Does the HIPAA Privacy Rule permit health care providers to obtain an electronic acknowledgement of the notice from individuals?

Answer

Yes. For notice delivered electrically, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice. A provider who gives his paper notice to a patient during a face-to-face encounter with the individual at first service delivery may also obtain an electronic acknowledgment from the individual, provided that the individual's acknowledgment is in writing. Thus, a receptionist's notation in the provider's computer system of the individual's receipt of the notice would not be considered a valid written acknowledgment of the individual.
Are health plans required to make a good faith effort to obtain from their enrollees a written acknowledgement of receipt of the notice?

Answer

No. Under the HIPAA Privacy Rule, only covered health care providers that have a direct treatment relationship with individuals are required to make a good faith effort to obtain the individual's acknowledgment of receipt of the notice. See 45 CFR 164.520(c)(2)(ii).
How are health care providers supposed to provide the notice to individuals and obtain their written acknowledgement of the notice when the first treatment encounter is over the phone or in some other manner that is not face-to-face?

Answer

The HIPAA Privacy Rule is intended to be flexible enough to address the various types of relationships that covered health care providers may have with the individuals they treat, including those treatment situations that are not face-to-face. For example, a health care provider who first treats a patient over the phone satisfies the notice provision requirements of the Privacy Rule by mailing the notice to the individual the same day, if possible. To satisfy the requirement that the provider also make a good faith effort to obtain the individual's acknowledgment of the notice, the provider may include a tear-off sheet or other document with the notice that requests that the acknowledgment be mailed back to the provider. The health care provider is not in violation of the Rule if the individual chooses not to mail back an acknowledgment; and a file copy of the form sent to the patient would be adequate documentation of the provider's good faith effort to obtain the acknowledgment.

Where a health care provider's initial contact with the patient is simply to schedule an appointment or a procedure, the notice provision and acknowledgment requirements may be satisfied at the time the individual arrives at the provider's facility for his or her appointment.

For service provided electronically, the notice must be sent electronically automatically and contemporaneously in response to the individual's first request for service. In this situation, an electronic return receipt or other return transmission from the individual is considered a valid written acknowledgment of the notice.

Last revised: March 26, 2007
We participate in an organized health care arrangement (OHCA). How are we to comply with the HIPAA Privacy Rule's requirements for providing notices and obtaining individuals' acknowledgements of the notice?

Answer

Health care providers and other covered entities that participate in an organized health care arrangement (OHCA) may use a single, joint notice that covers all of the participating covered entities (provided that the conditions at 45 CFR 164.520(d) are met), or may each maintain separate notices. Where a joint notice is provided to an individual by any one of the covered entities to which the joint notice applies, the Privacy Rule’s requirements for providing the notice are satisfied for all others covered by the joint notice. If the joint notice is provided to an individual by a direct treatment provider participating in the OHCA, the provider must make a good faith effort to obtain the individual’s written acknowledgment of receipt of the joint notice. Where the joint notice is provided to the individual by a participating covered entity other than a direct treatment provider, no acknowledgment need be obtained.

However, where covered entities participating in an OHCA choose to maintain separate notices, each covered entity from which an individual obtains services must provide its notice to the individual in accordance with the applicable requirements of 45 CFR 164.520(c). In addition, each direct treatment provider within the OHCA must make a good faith effort to obtain the individual’s acknowledgment of the notice he or she provides.
Does a health plan have to provide a copy of its notice to each dependent receiving coverage under a policy?

Answer

No. A health plan satisfies the HIPAA Privacy Rule's requirements for providing the notice by distributing its notice only to the named insured of a policy under which coverage is provided both to the named insured and his or her dependents. See 45 CFR 164.520(c)(1)(iii).
For group health plan products, can the health plan send its notice to the administrator of the group product or the plan sponsor for them to distribute to each employee enrolled in the plan?

Answer

The HIPAA Privacy Rule requires a health plan to distribute its notice to each individual covered by the plan. Health plans may arrange to have another person or entity, for example, a group administrator or a plan sponsor, distribute the notice on their behalf. However, if the other person or entity fails to distribute the notice to the plan’s enrollees, the health plan may be in violation of the Privacy Rule.

Last revised: March 26, 2007
Are health care providers required by the HIPAA Privacy Rule to post their entire notice at their facility or may they post just a brief description of the notice?

Answer

Covered health care providers that maintain an office or other physical site where they provide health care directly to individuals are required to post their entire notice at the facility in a clear and prominent location. The Privacy Rule, however, does not prescribe any specific format for the posted notice, just that it include the same information that is distributed directly to the individual. Covered health care providers have discretion to design the posted notice in a manner that works best for their facility, which may be to simply post a copy of the pages of the notice that is provided directly to individuals.
Can a covered entity bypass obtaining an individual's authorization for a use or disclosure not permitted by the HIPAA Privacy Rule simply by informing individuals of the use or disclosure through its notice of privacy practices?

Answer:

No. A covered entity's notice is not a substitute for an individual's authorization. Covered entities are required to obtain the individual's written authorization for any use or disclosure of protected health information not permitted or required by the Privacy Rule. See 45 CFR 164.508. Simply including in the notice a description of such a use or disclosure does not obviate the need for the covered entity to obtain the individual's prior written authorization, when that authorization is required by the Rule. Instead, the notice must reflect the uses and disclosures a covered entity may make without the individual's authorization, as permitted by Privacy Rule, as well as state that any other uses or disclosures only will be made with the individual's written authorization. See 45 CFR 164.520(b).
Is our medical practice required to notify patients through the mail of any changes to our notice?

Answer

No. The HIPAA Privacy Rule does not require a covered health care provider to mail out its revised notice or otherwise notify patients by mail of changes to the notice. Rather, when a covered health care provider with a direct treatment relationship with individuals makes a change to his notice, he must make the notice available upon request to patients or other persons on or after the effective date of the revision, and, if he maintains a physical service delivery site, post the revised notice in a clear and prominent location in his facility. See 45 CFR 164.520(c)(2)(iv). In addition, the provider must ensure that the current notice, in effect at that time, is provided to patients at first service delivery, and made available on his customer service web site, if he has one. See 45 CFR 164.520(c).
Is a physician required to give her notice to every patient or can she just post the notice in her waiting room and give a copy to those patients who ask for it?

Answer

The HIPAA Privacy Rule requires a covered health care provider with direct treatment relationships with individuals to give the notice to every individual no later than the date of first service delivery to the individual and to make a good faith effort to obtain the individual’s written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where she provides health care directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy. See 45 CFR 164.520(c) for other notice provision requirements.
It is common for hospitals and other health care providers to collect preoperative information over the phone from a new patient prior to the day of surgery in order to determine whether the patient has any special medical concerns or issues that need to be addressed. Does the HIPAA Privacy Rule prohibit this practice if the patient has not yet received or acknowledged the provider's notice?

Answer

No, the Privacy Rule does not prohibit this practice. Where a health care provider's initial contact with a patient is simply to schedule an appointment or a procedure, or to collect information in anticipation of an appointment or a procedure, the Privacy Rule's requirements for providing the notice and obtaining a patient's acknowledgment of the notice may be satisfied at the time the individual arrives at the provider's facility for his or her appointment or procedure.
Is a pharmacist permitted to have customer acknowledge receipt of the notice by signing or initialing the log book that they already sign when they pick up prescriptions?

Answer

Yes, provided that the individual is clearly informed on the log book of what they are acknowledging and the acknowledgment is not also used as a waiver or permission for something else that also appears on the log book (such as a waiver to consult with the pharmacist). The HIPAA Privacy Rule provides covered health care providers with discretion to design an acknowledgment process that works best for their businesses.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule require my doctor to send my medical records to the government?

Answer

No. The Rule does not require a physician or any other covered entity to send medical information to the government for a government database or similar operation. This Rule does not require or allow any new government access to medical information, with one exception: the Rule does give the Department of Health and Human Services Office for Civil Rights (OCR) the authority to investigate complaints that Privacy Rule protections or rights have been violated, and otherwise to ensure that covered entities comply with the Rule.

For enforcement purposes, OCR may need to look at how a covered entity handled medical records and other personal health information, as is typical in many enforcement settings. This investigative authority is needed so that the Rule can be enforced, and to ensure the independent review of consumers’ concerns over privacy violations. Even so, the Privacy Rule limits disclosures to OCR to information that is “pertinent to ascertaining compliance.” OCR will maintain stringent controls to safeguard any individually identifiable health information that it receives. If covered entities could avoid or ignore enforcement requests, consumers would not have a way to ensure an independent review of their concerns about privacy violations under the Rule.

Last revised: April 03, 2007
Why would a HIPAA Privacy Rule require covered entities to turn over anybody's personal health information as part of a government enforcement process?

Answer

An important ingredient in ensuring compliance with the Privacy Rule is the Department of Health and Human Services' (HHS) responsibility to investigate complaints that the Rule has been violated and to follow up on other information regarding noncompliance. At times, this responsibility entails seeing personal health information, such as when an individual indicates to the Department that they believe a covered entity has not properly handled their medical records.

What information would be needed depends on the circumstances and the alleged violations. The Privacy Rule limits HHS Office for Civil Rights' (OCR) access to information that is "pertinent to ascertaining compliance." In some cases, no personal health information may be needed. For instance, OCR would need to review only a business contract to determine whether a health plan included appropriate language to protect privacy when it hired an outside company to help process claims.

Examples of investigations that may require OCR to have access to protected health information include:

- Allegations that a covered entity refused to note a request for correction in a patient's medical record, or did not provide complete access to a patient's medical records to that patient.

- Allegations that a covered entity used health information for marketing purposes without first obtaining the individuals' authorization when required by the Rule. OCR may need to review information in the marketing department that contains personal health information, to determine whether a violation has occurred.
Will this HIPAA Privacy Rule make it easier for police and law enforcement agencies to get my medical information?

Answer

No. The Rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists, since the Rule establishes new procedures and safeguards that restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the Rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires covered entities to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement.

In most States, such permission is not required today. Where State law imposes additional restrictions on disclosure of health information to law enforcement, those State laws continue to apply. This Rule sets a national floor of legal protections; it is not a set of “best practices.” Even in those circumstances when disclosure to law enforcement is permitted by the Rule, the Privacy Rule does not require covered entities to disclose any information. Some other Federal or State law may require a disclosure, and the Privacy Rule does not interfere with the operation of these other laws. However, unless the disclosure is required by some other law, covered entities should use their professional judgment to decide whether to disclose information, reflecting their own policies and ethical principles. In other words, doctors, hospitals, and health plans could continue to follow their own policies to protect privacy in such instances.
Does the HIPAA Privacy Rule create a government database with all individuals' personal health information?

Answer

No. The Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
How does the HIPAA Privacy Rule affect my rights under the Federal Privacy Act?

Answer

The Privacy Act of 1974 (U.S. Department of Justice) protects personal information about individuals held by the Federal government. Covered entities that are Federal agencies or Federal contractors that maintain records that are covered by the Privacy Act not only must obey the Privacy Rule’s requirements, but also must comply with the Privacy Act.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.

Last revised: March 28, 2007
If I believe that my privacy rights have been violated, when can I submit a complaint?

Answer

By law, health care providers (including doctors and hospitals) who engage in certain electronic transactions, health plans, and health care clearinghouses, (collectively, "covered entities") have until April 14, 2003, to comply with the HIPAA Privacy Rule. (Small health plans have until April 14, 2004, to comply). Activities occurring before April 14, 2003, are not subject to the Office for Civil Rights (OCR) enforcement actions. After that date, a person who believes a covered entity is not complying with a requirement of the Privacy Rule may file with OCR a written complaint, either on paper or electronically. This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred. The Secretary may waive this 180-day time limit if good cause is shown. See 45 CFR 160.306 and 164.534. OCR will provide further information on its web site about how to file a complaint (www.hhs.gov/ocr/hipaa/).

In addition, after the compliance dates above, individuals have a right to file a complaint directly with the covered entity. Individuals should refer to the covered entity's notice of privacy practices for more information about how to file a complaint with the covered entity.
If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?

Answer

The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See 45 CFR 164.524.
Does the HIPAA Privacy Rule protect genetic information?

Answer

Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse. See 45 C.F.R 160.103 and 164.501.

Last revised: May 24, 2007
Can a physician's office FAX patient medical information to another physician's office?

Answer

The HIPAA Privacy Rule permits physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other physician's office, and placing the fax machine in a secure location to prevent unauthorized access to the information. See 45 CFR 164.530(c).

For more detailed information about health privacy, you may want to visit our [Medical Privacy: National Standards to Protect the Privacy of Personal Health Information](http://www.hhs.gov/) site and our full set of [Frequently Asked Questions](http://www.hhs.gov/hipaafaq/providers/smaller/356.html).

Last revised: March 26, 2007
Are hospitals able to inform the clergy about parishioners in the hospital?

Answer

Yes, the HIPAA Privacy Rule allows this communication to occur, as long as the patient has been informed of this use and disclosure, and does not object. The Privacy Rule provides that a hospital or other covered health care provider may maintain in a directory the following information about that individual: the individual's name; location in the facility; health condition expressed in general terms; and religious affiliation. The facility may disclose this directory information to members of the clergy. Thus, for example, a hospital may disclose the names of Methodist patients to a Methodist minister unless a patient has restricted such disclosure. Directory information, except for religious affiliation, may be disclosed only to other persons who ask for the individual by name. When, due to emergency circumstances or incapacity, the patient has not been provided an opportunity to agree or object to being included in the facility's directory, these disclosures may still occur, if such disclosure is consistent with any known prior expressed preference of the individual and the disclosure is in the individual's best interest as determined in the professional judgment of the provider. See 45 CFR 164.510(a).
My State requires consent to use or disclose health information. Does the HIPAA Privacy Rule take away this protection?

Answer

No. The Privacy Rule does not prohibit a covered entity from obtaining an individual's consent to use or disclose his or her health information and, therefore, presents no barrier to the entity's ability to comply with State law requirements.

Last revised: April 03, 2007
Are the following types of insurance covered under HIPAA: long/short term disability; workers’ compensation; automobile liability that includes coverage for medical payments?

Answer

No, the listed types of policies are not health plans. The HIPAA Administrative Simplification regulations specifically exclude from the definition of a “health plan” any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits, which are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). See 45 CFR 160.103. As described in the statute, excepted benefits are one or more (or any combination thereof) of the following policies, plans or programs:

- Coverage only for accident, or disability income insurance, or any combination thereof.

- Coverage issued as a supplement to liability insurance.

- Liability insurance, including general liability insurance and automobile liability insurance.

- Workers’ compensation or similar insurance.

- Automobile medical payment insurance.

- Credit-only insurance.

- Coverage for on-site medical clinics

- Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

Last revised: April 03, 2007
Is an entity that is acting as a third party administrator to a group health plan a covered entity?

Answer

No, providing services to or acting on behalf of a health plan does not transform a third party administrator (TPA) into a covered entity. Generally, a TPA of a group health plan would be acting as a business associate of the group health plan. Of course, the TPA may meet the definition of a covered entity based on its other activities (such as by providing group health insurance). See 45 CFR 160.103.

Last revised: April 03, 2007
The Social Security Administration (SSA) collects medical records when making disability determinations for both title II (Disability Insurance) and title XVI (Supplemental Security Income, SSI) of the Social Security Act. Is SSA a covered entity (e.g., a health plan)?

Answer

The SSA is not a covered entity. The collection of individually identifiable health information is not a factor in determining whether an entity is a covered entity. Covered entities are defined in HIPAA; they are (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transactions Rule. SSA meets none of these criteria as defined at 45 CFR 160.103.
Is the Privacy Rule compliance date delayed by the Administrative Simplification Compliance Act (ASCA) that was enacted in December 2001?

Answer

No, the compliance dates for the Privacy Rule is April 14, 2003, or, for small health plans, April 14, 2004. ASCA does not apply to the HIPAA Privacy Rule. Rather, ASCA delays compliance with the Transaction and Code Set standards adopted by the HIPAA Transactions Rule for covered entities that file a compliance plan. More information about ASCA can be found on the web site for the Centers for Medicare and Medicaid Services at http://cms.hhs.gov/hipaa/.

Last revised: April 03, 2007
HIPAA allows "small health plans," defined as health plans having annual receipts of $5 million or less, an additional year (in the case of the Privacy Rule, until April 14, 2004) to come into compliance. How should a health plan determine what receipts to use to decide whether it qualifies as a "small health plan?"

Answer

Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 CFR 121.104 to calculate annual receipts. Health plans that do not report receipts to the IRS - for example, ERISA group health plans that are exempt from filing income tax returns - should use proxy measures to determine their annual receipts. Further information about the relevant provisions of 13 CFR 121.104 and these proxy measures, and additional information related to "small health plans," may be found at http://cms.hhs.gov/hipaa/hipaa2/default.asp.

Last revised: March 30, 2007
Does the HIPAA Privacy Rule require that covered entities provide patients with access to oral information?

Answer

No. The Privacy Rule requires covered entities to provide individuals with access to protected health information about themselves that is contained in their "designated record sets." The term "record" in the term "designated record set" does not include oral information; rather, it connotes information that has been recorded in some manner.

The Rule does not require covered entities to tape or digitally record oral communications, nor retain digitally or tape recorded information after transcription. But if such records are maintained and used to make decisions about the individual, they may meet the definition of "designated record set." For example, a health plan is not required to provide a member access to tapes of a telephone "advice line" interaction if the tape is maintained only for customer service review and not to make decisions about the member.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule require that covered entities document all oral communications?

Answer

No. The Privacy Rule does not require covered entities to document any information, including oral information, that is used or disclosed for treatment, payment or health care operations.

The Rule includes, however, documentation requirements for some information disclosures for other purposes. For example, some disclosures must be documented in order to meet the standard for providing a disclosure history to an individual upon request. Where a documentation requirement exists in the Rule, it applies to all relevant communications, whether in oral or some other form. For example, if a covered physician discloses information about a case of tuberculosis to a public health authority as permitted by the Rule at 45 CFR 164.512, then he or she must maintain a record of that disclosure regardless of whether the disclosure was made orally, by phone, or in writing.

For more detailed information about health privacy, you may want to visit our Medical Privacy: National Standards to Protect the Privacy of Personal Health Information site and our full set of Frequently Asked Questions.
Does the HIPAA Privacy Rule require a business associate to create a notice of privacy practices?

Answer

No. However, a covered entity must ensure through its contract with the business associate that the business associate's uses and disclosures of protected health information and other actions are consistent with the covered entity's privacy policies, as stated in covered entity's notice. Also, a covered entity may use a business associate to distribute its notice to individuals.

Last revised: April 03, 2007
Does the HIPAA Privacy Rule permit covered entities to disclose protected health information, without individuals' authorization, to public officials responding to a bioterrorism threat or other public health emergency?

Answer

Yes. The Rule recognizes that various agencies and public officials will need protected health information to deal effectively with a bioterrorism threat or emergency. To facilitate the communications that are essential to a quick and effective response to such events, the Privacy Rule permits covered entities to disclose needed information to public officials in a variety of ways. Covered entities may disclose protected health information, without the individual's authorization, to a public health authority acting as authorized by law in response to a bioterrorism threat or public health emergency (see 45 CFR 164.512(b), public health activities). The Privacy Rule also permits a covered entity to disclose protected health information to public officials who are reasonably able to prevent or lessen a serious and imminent threat to public health or safety related to bioterrorism (see 45 CFR 164.512(j), to avert a serious threat to health or safety). In addition, disclosure of protected health information, without the individual's authorization, is permitted where the circumstances of the emergency implicates law enforcement activities (see 45 CFR 164.512(f)); national security and intelligence activities (see 45 CFR 164.512(k)(2)); or judicial and administrative proceedings (see 45 CFR 164.512(e)).
Does the HIPAA Privacy Rule permit nursing homes and other health care institutions to disclose information concerning admissions of supplemental security income (SSI) recipients to the Social Security Administration (SSA)?

Answer

Yes. SSA requires nursing homes, extended care facilities, and intermediate care facilities to report to SSA, within 2 weeks, admissions information about anyone receiving SSI who is admitted to the institution. The purpose of these reporting requirements is to prevent SSI overpayments caused by a SSI recipient’s failure to timely report changes in eligibility. These requirements are stated in the Social Security Act (42 U.S.C. 1383(e)(1)(C)), and communicated through SSA’s guidance and other implementation materials. The Privacy Rule permits covered entities to disclose protected health information without the individual’s authorization as required to comply with this law. See 45 CFR 164.512(a).

Last revised: April 03, 2007
Does the HIPAA Privacy Rule preempt State laws?

Answer

The HIPAA Privacy Rule provides a Federal floor of privacy protections for individuals' individually identifiable health information where that information is held by a covered entity or by a business associate of the covered entity. State laws that are contrary to the Privacy Rule are preempted by the Federal requirements, unless a specific exception applies. These exceptions include if the State law (1) relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information, (2) provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) requires certain health plan reporting, such as for management or financial audits. In these circumstances, a covered entity is not required to comply with a contrary provision of the Privacy Rule.

In addition, the Department of Health and Human Services (HHS) may, upon specific request from a State or other entity or person, determine that a provision of State law which is "contrary" to the Federal requirements – as defined by the HIPAA Administrative Simplification Rules – and which meets certain additional criteria, will not be preempted by the Federal requirements. Thus, preemption of a contrary State law will not occur if the Secretary or designated HHS official determines, in response to a request, that one of the following criteria apply: the State law (1) is necessary to prevent fraud and abuse related to the provision of or payment for health care, (2) is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation, (3) is necessary for State reporting on health care delivery or costs, (4) is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or (5) has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

It is important to recognize that only State laws that are "contrary" to the Federal requirements are eligible for an exemption determination. As defined by the Administrative Simplification Rules, contrary means that it would be impossible for a covered entity to comply with both the State and Federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.


Download Acrobat Reader to view and print PDF files
How does the HIPAA Privacy Rule reduce the potential for conflict with State laws?

Answer

The Privacy Rule is designed to minimize conflicts between Federal requirements and those of State law in the following ways:

- The Privacy Rule establishes a floor of Federal privacy protections and individual rights with respect to individually identifiable health information held by covered entities and their business associates. Covered entities may provide greater privacy rights to individuals and greater protections on such information. In addition, covered entities may comply with State laws that provide greater protections for individually identifiable health information and greater privacy rights for individuals.

- The Privacy Rule permits a covered entity to use or disclose protected health information if a State law requires the use or disclosure. See 45 C.F.R. 164.512(a).

- The Privacy Rule permits a covered entity to disclose protected health information to a public health authority who is authorized by law to collect such information for the purposes of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. (See 45 C.F.R. 164.512(b) for all of the public health disclosures permitted by the Privacy Rule.) Thus, State laws that provide for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation, or intervention, likely will not conflict with the Privacy Rule. In the unusual case where there is a conflict, the State law would stand. See 45 C.F.R. 160.203(c). Because the Administrative Simplification Rules themselves exempt such State laws from preemption, a request for the Department of Health and Human Services (HHS) to issue a preemption exception determination is unnecessary and inappropriate.

- The Privacy Rule permits a covered entity to disclose protected health information to a health oversight agency for oversight activities authorized by law, such as audits and licensure activities. See 45 C.F.R. 164.512(d). Thus, State laws that provide for certain health plan reporting for the purpose of management or financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals, likely will not conflict with the Privacy Rule. In the unusual case where there is a conflict, the State law would stand. See 45 C.F.R. 160.203(d). Because the Administrative Simplification Rules themselves exempt such State laws from preemption, a request for the Department of Health and Human Services (HHS) to issue a preemption exception determination is unnecessary and inappropriate.

An unofficial version of the Privacy Rule and the preemption requirements may be accessed at http://www.hhs.gov/ocr/combinedregtext.pdf (PDF - 2.8MB).

Download Acrobat Reader to view and print PDF files.

Last revised: June 21, 2007
How do I know if a State law is "contrary" to the HIPAA Privacy Rule?

Answer

A State law is "contrary" to the HIPAA Privacy Rule if it would be impossible for a covered entity to comply with both the State law and the Federal Privacy Rule requirements, or if the State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. See the definition of "contrary" at 45 C.F.R. 160.202. For example, a State law that prohibits the disclosure of protected health information to an individual who is the subject of the information may be contrary to the Privacy Rule, which requires the disclosure of protected health information to an individual in certain circumstances. With certain exceptions, the Privacy Rule preempts "contrary" State laws. See 45 C.F.R. Part 160, Subpart B, which may be accessed (in unofficial version) at http://www.hhs.gov/ocr/combinedregtext.pdf (PDF - 2.8MB).

Download Acrobat Reader to view and print PDF files.
How do I know if a State law is "more stringent" than the HIPAA Privacy Rule?

Answer

In general, a State law is "more stringent" than the HIPAA Privacy Rule if it relates to the privacy of individually identifiable health information and provides greater privacy protections for individuals' identifiable health information, or greater rights to individuals with respect to that information, than the Privacy Rule does. See the definition of "more stringent" at 45 C.F.R. 160.202 for the specific criteria. For example, a State law that provides individuals with a right to inspect and obtain a copy of their medical records in a more timely manner than the Privacy Rule is "more stringent" than the Privacy Rule.

In the unusual case where a more stringent provision of State law is contrary to a provision of the Privacy Rule, the Privacy Rule provides an exception to preemption for the more stringent provision of State law, and the State law prevails. Where the more stringent State law and Privacy Rule are not contrary, covered entities must comply with both laws.


Download Acrobat Reader to view and print PDF files.

Last revised: June 21, 2007
Under what circumstances will HHS grant a State law preemption exception determination?

Answer

The Department of Health and Human Services (HHS) may, upon specific request from a State or other entity or person, issue a determination that a contrary State law which meets certain criteria will not be preempted by the Federal requirements. Only State laws that are "contrary" to the Federal requirements are eligible for an exemption determination. As defined by HIPAA's Administrative Simplification Rules, "contrary" means that it would be impossible for a covered entity to comply with both the State and Federal requirements, or that the State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. See 45 C.F.R. 160.202.

A contrary State law is not preempted by the Federal requirements if the Secretary or designated HHS official determines that the request meets one or more of the following criteria, which are set forth in 45 C.F.R. 160.203(a):

1. The provision of State law is necessary
   - to prevent fraud and abuse related to the provision of or payment for health care,
   - to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,
   - for State reporting on health care delivery and costs, or
   - for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

2. The principal purpose of the provision of State law is to regulate the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

Thus, States and other persons may request in writing that HHS except certain contrary provisions of State law from preemption by the Privacy Rule. The request for exception must explain how the State law in question is actually contrary to the Federal requirements, and how the contrary State law meets one or more of the specific criteria for which exceptions may be granted. Title 45 C.F.R. Part 160, Subpart B, sets forth the specific requirements related to preemption of State law and the criteria and process for requesting exception determinations.

HHS will not make determinations as to whether a provision of State law is "more stringent" than a provision of the HIPAA Privacy Rule, and will not determine whether a provision is "contrary" to the Privacy Rule, except in the context of, and as necessary to, making an exception determination.

See 45 C.F.R. Part 160, Subpart B, for specific requirements related to preemption of State law. An unofficial version of the Privacy Rule and the preemption requirements

http://www.hhs.gov/hipaafaq/state/404.html

8/28/2007
Under what circumstances will HHS grant a State law preemption exception determination?


Download Acrobat Reader to view and print PDF files

Last revised: June 21, 2007
My State law provides greater privacy protections on patients’ HIV information than the HIPAA Privacy Rule. Is this more protective State law preempted by the Privacy Rule?

Answer:

No. The Privacy Rule establishes a floor of Federal privacy protections and rights for individuals. If a provision of State law provides greater privacy protection than a provision of the Privacy Rule, and it is possible to comply with both the State law and the Privacy Rule (e.g., where a State law prohibits the disclosure of HIV status while the Privacy Rule permits such disclosure), there is no conflict between the State law and the Privacy Rule, and no preemption.

Further, even in the unusual case where a "more stringent" provision of a State law is "contrary" to a provision of the Privacy Rule – that is, it is impossible to comply with both the Privacy Rule and the State law, or the State law is an obstacle to accomplishing the full purposes and objectives of HIPAA’s Administrative Simplification provisions – the Administrative Simplification Rules specifically provide an exception to preemption of State law. Thus, if a more stringent provision of State law protects HIV patient information and is contrary to the Privacy Rule, the "more stringent" State law would prevail. Because HIPAA’s Administrative Simplification Rules themselves except more stringent, contrary State law from preemption, it is neither necessary nor appropriate to request a preemption exception determination from the Department of Health and Human Services.

My State law authorizes health care providers to report suspected child abuse to the State Department of Health and Social Services. Does the HIPAA Privacy Rule preempt this State law?

Answer

No. The Privacy Rule permits covered health care providers and other covered entities to disclose reports of child abuse or neglect to public health authorities or other appropriate government authorities. See 45 C.F.R. 164.512(b)(1)(ii). Thus, there is no conflict between the State law and the Privacy Rule, and no preemption. Covered entities may report such information and be in compliance with both the State law and the Privacy Rule.

Further, even in the unusual case where a State law that provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention is contrary to a provision of the Privacy Rule – that is, it is impossible for a covered entity to comply with both the Privacy Rule and the State law, or the State law is an obstacle to accomplishing the full purposes and objectives of HIPAA’s Administrative Simplification provisions – the Administrative Simplification Rules specifically provide an exception to preemption of State law. Thus, if a provision of State law provided for public health surveillance and was contrary to the Privacy Rule, the State law would prevail. Because the Administrative Simplification Rules except such contrary State laws from preemption, it is neither necessary nor appropriate to request a preemption exception determination from the Department of Health and Human Services. See 45 C.F.R. 160.202 for the definition of "contrary" and 45 C.F.R. 160.203 for the general rule and exceptions to preemption. An unofficial version of the Privacy Rule and the preemption requirements may be accessed at http://www.hhs.gov/ocr/combinedregtext.pdf (PDF - 2.8MB).
Will a State law preemption exception determination apply only to the entity that requested the determination?

Answer

No. Preemption exception determinations issued by the Department of Health and Human Services (HHS) will apply generally to all persons subject to the particular provision of State law for which the exception was granted. When an exception determination is made, HHS will promptly inform the public through publication of notice in the Federal Register, and on HHS' web sites, including the OCR Privacy web site at http://www.hhs.gov/ocr/hipaa/.

Last revised: April 03, 2007

http://www.hhs.gov/hipaafaq/state/407.html

8/28/2007
Will HHS make determinations as to whether a provision of State law is “more stringent” than or “contrary” to a provision of the HIPAA Privacy Rule?

Answer

The Department of Health and Human Services (HHS) will not make determinations as to whether a provision of State law is "more stringent" than a provision of the Privacy Rule. HIPAA's Administrative Simplification Rules provide a general exception to preemption for more stringent, contrary State laws. Because such an exception already exists, it is neither necessary nor appropriate to request a preemption exception determination from HHS. Further, HHS will not determine whether a provision is "contrary" to the Privacy Rule, except in the context of, and as necessary to, making an exception determination for State laws that meet one or more of the criteria listed at 45 CFR 160.203(a). See 45 C.F.R. 160.202 for the definitions of "more stringent" and "contrary." An unofficial version of the Privacy Rule and the preemption requirements may be accessed at http://www.hhs.gov/ocr/combinedregtext.pdf (PDF - 2.8MB).

Download Acrobat Reader to view and print PDF files.
Will HHS publish exception determinations?

Answer

Yes. The Department of Health and Human Services (HHS) will promptly inform the public of exception determinations through publication of notice in the Federal Register, and on HHS' web sites, including the OCR Privacy web site at http://www.hhs.gov/ocr/hipaa/.

Last revised: June 21, 2007
Is a flexible spending account or a cafeteria plan a covered entity for purposes of the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards?

Answer

A "group health plan" is a covered entity under the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards. A "group health plan" is defined as an "employee welfare benefit plan," as that term is defined by the Employee Retirement Income Security Act (ERISA), to the extent that the plan provides medical care. See 42 USC § 1320d(5)(A) and 45 CFR 160.103. Thus, to the extent that a flexible spending account or a cafeteria plan meets the definition of an employee welfare benefit plan under ERISA and pays for medical care, it is a group health plan, unless it has fewer than 50 participants and is self-administered. Employee welfare benefit plans with fewer than 50 participants and that are self-administered are not group health plans. Flexible spending accounts and cafeteria plans are not excluded from the definition of "health plan" as excepted benefits. See 45 CFR 160.103, paragraph (2)(i) of the definition of "health plan."

Last revised: March 26, 2007
Does the Privacy Rule permit health plans to disclose protected health information to pharmaceutical manufacturers for the adjudication of drug rebate contracts?

Answer

Yes. The Privacy Rule permits a health plan to disclose protected health information, such as prescription numbers, to a pharmaceutical manufacturer for purposes of adjudicating claims submitted under a drug rebate contract. Because the amount of the rebate is based on drug utilization by individual enrollees, such disclosures are permitted as part of a covered entity’s payment activities. See 45 CFR 164.502(a)(1)(ii) and the definition of “payment” at 45 CFR 164.501. A business associate agreement is not required to make these disclosures. However, a health plan must make reasonable efforts to limit the information disclosed to that which is the minimum necessary to adjudicate claims under the contract. See 45 CFR 164.502(b) and 164.514(d) for more information on the minimum necessary standard.
Does the Privacy Rule permit State Medicaid agencies to disclose protected health information to pharmaceutical manufacturers and third party data vendors for purposes of validating claims under the Medicaid Drug Rebate program?

Answer

Yes. The Privacy Rule permits State Medicaid agencies to disclose protected health information, such as prescription numbers, to pharmaceutical manufacturers and third party data vendors that assist the pharmaceutical manufacturers, for purposes of validating claims submitted under the Medicaid Drug Rebate program. Because the amount of the rebate is based on drug utilization by individual enrollees, such disclosures are permitted as part of a State Medicaid agency's payment activities. See 45 CFR 164.502(a)(1)(ii) and the definition of "payment" at 45 CFR 164.501. A business associate agreement is not required to make these disclosures. State Medicaid agencies are required by law to disclose certain information to drug manufacturers as part of the drug rebate program. To the extent that the law requires a disclosure, the minimum necessary standard does not apply. (See 45 CFR 164.512(a) for further information and limitations on disclosures required by law.) To the extent that protected health information is disclosed for payment purposes but not pursuant to a legal requirement, the State Medicaid agency must make reasonable efforts to limit that information to that which is the minimum necessary to adjudicate the rebate claims. See 45 CFR 164.502(b) and 164.514(d) for more information on the minimum necessary standard.
Must a covered entity with a Notice of Privacy Practices that reflects more stringent State laws of multiple States, revise the whole Notice every time one State law materially changes?

Answer

The Privacy Rule requires the Notice of Privacy Practices (Notice) to identify, among other things, what uses and disclosures the covered entity may make of protected health information. The Notice must reflect any State law(s) that is more stringent than the Privacy Rule with respect to the use or disclosure of this information. Where the covered entity is subject to the privacy laws of multiple States, the more stringent use and disclosure laws of each of the States, if any, must be reflected in the Notice. See 45 CFR 164.520(b)(1)(ii)(C). When there is a material revision to the Notice based on a change in State law, covered entities must use the revised Notice to meet the Rule’s requirements for distribution of the Notice that occur on or after the effective date of the revised Notice. See, generally, §§164.520(c)(1)-(3). In particular, a health plan must provide individuals (in most cases, the named insured) then covered by the plan with the revised Notice within 60 days of the revision. See §164.520(c)(1)(i)(C).

The Notice requirements are intended to ensure that individuals are fairly informed about how a covered entity may use or disclose their personal health information, including important limitations imposed by State law. Although a covered entity can describe more stringent State privacy laws in the uses and disclosures section of its Notice, this may be more confusing than informative to the individual, particularly where multiple and varying State laws may be applicable. There are other ways a covered entity can design its Notice that may make this information easier for the individual to read and understand, as well as to facilitate the covered entity’s ability to keep the information current and accurate. For instance, a general statement could be included in the uses and disclosures section of the Notice that clearly identifies and refers the reader to a separate section of the Notice which describes the more stringent State privacy law(s) and more fully informs the reader about how protected health information may be used and disclosed. Thus, when more stringent State privacy laws materially change the covered entity’s privacy practices, the covered entity would need to revise only the section of the Notice that contains the State law specific information.

Having a separable section on more stringent State laws can also facilitate distribution of the revised Notice when material changes occur in this section of the Notice. The revised State law section, if on a separate page, may be more readily inserted in or associated with existing Notices in place of the out-dated material.
To provide individuals with an accounting for disclosures, does a covered entity have to document each medical record that may be accessed by a public health authority in the course of surveillance activities that involve all patient records?

Answer

The Privacy Rule does not require a notation in each medical record that has been accessed by public health authorities, as long as the information required under the Privacy Rule is included in the accounting for disclosures. Where, as with many public health disclosures, access to an entire universe of records is involved, tracking disclosures can be accomplished without the need for documentation in each record. This flexibility in the manner of documentation facilitates complying with the accounting requirement.

By way of background, a covered entity may disclose protected health information (PHI) without the patient’s authorization to a public health authority that is legally permitted to collect or receive such information for public health surveillance or related activities (45 CFR 164.512(b)(1)). A covered entity is also required by the Privacy Rule to account to the patient for such disclosures of PHI, if the patient asks (45 CFR 164.528). Further, under the Privacy Rule, making a set of records available for review by a third party constitutes a “disclosure” of the PHI in the entire set of records, regardless of whether the third party actually reviews any particular record. See 45 CFR 164.501, for the definition of disclosure. Thus, mere access by a third party, such as a public health authority, to PHI is a disclosure and subject to an accounting for disclosures.

Public health surveillance activities often involve a retrospective review by a public health authority of a universe of patient records to identify reportable events. When a reportable case is identified, the specific data items pertinent to the public health surveillance activity are extracted and reported to the public health authority. For example, retrospective review of the medical charts for all patients treated by a health care provider or all charts of patients treated in the entity’s emergency department may be required to identify cases of new or previously unknown infectious agents, clinical conditions associated with the use or abuse of illicit or prescription drugs, or adverse events or reactions associated with pharmaceuticals or medical devices. In these cases, as noted above, all records to which access was provided to the public health authority are deemed to have been disclosed under the Privacy Rule. Because of the universal nature of the access provided, the documentation required for the disclosure can be easily maintained. The covered entity need only document the identity (and address if known) of the public health authority to which access was provided, a description of the records and PHI subject to access, the purpose for the disclosure, and when access was provided. This documentation need not be noted in each record. It would be sufficient, for instance, for the covered entity to maintain a separate notation of such disclosures, applicable to all records so accessed. Then, if an individual requests an accounting, the covered entity need only determine whether the individual’s records were among the universe.
of records to which the public health authority was granted access. All individuals
whose records were accessed in this fashion would receive the same accounting for
the disclosure.

For example, if on August 1, 2003, a hospital began providing a public health
authority ongoing access to the medical charts of all patients treated in its
emergency department to identify reportable cases and extract relevant information
required for a particular surveillance activity, it would be sufficient, under §164.528
(b)(2), for the accounting to include the following:

- the identity, and address, if known, of the public health authority;
- a statement that the public health authority had access to medical charts for
  patients treated in the emergency department;
- the date (or approximate range of dates) when the individual’s record was
  subject to access (e.g., access provided within a week of treatment in ER on [fill
  in date of individual visit]); and
- a statement of the purpose of the access (e.g., identify the particular public
  health surveillance activity).

The same basic statement could then be provided in response to a request for an
accounting by any individual who was seen in the emergency department of the
hospital on or after August 1, 2003.
How can a covered entity account for the date of access if it is not known for certain?

Answer

Accounting for disclosures requires an individual to be informed of the date the disclosure was made (45 CFR 164.528(b)(2)). If access to a universe of records was provided for a discrete period of time, OCR interprets this provision to permit the accounting to include the range of dates (e.g., access was provided from August 1 to August 3, 2003; or during the week of August 10, 2003). If the disclosure is routinely made within a set period from an event, OCR, likewise, interprets this provision to permit the accounting to provide the date of the event and the normal interval (e.g., gunshot wound reported within 48 hours of treatment and provide date of treatment; hospital discharges reported on 15th of the following month and provide date of discharge; or access provided to public health authorities within 30 days of treatment in emergency department and provide the date of treatment).
May a covered entity hire a business associate to create a limited data set, and may the public health authority be a business associate for that purpose, even if the public health authority is also the intended recipient of the limited data set?

Answer

A covered entity may enter into a business associate agreement with the public health authority for the sole purpose of creating a limited data set, even if the same public health authority is also the intended recipient of the information (45 CFR 164.514(e)(3)(ii)). For example, the covered entity may contract with the public health authority as a business associate for the exclusive purpose of reviewing medical charts and extracting the facially unidentifiable information needed for the particular public health surveillance activity. In these cases, the public health authority, as the covered entity’s business associate for purposes of creating a limited data set, must agree to return, destroy or not remove from the covered entity’s premises the protected health information that includes the direct identifiers, once the public health authority has completed the conversion of the information into a limited data set for its own public health use. Because the public health authority is not only the covered entity’s business associate for creating the limited data set, but also the intended recipient of the limited data set, the public health authority must enter into both a data use agreement and a business associate agreement. The data use agreement can be combined with the business associate agreement into a single agreement so long as the agreement meets the requirements of both provisions. See 45 CFR 164.504(e)(2) and 164.514(e)(4).

While there are two disclosures in this case – the disclosure to the public health authority in its role as the covered entity’s business associate in creating the limited data set, and the disclosure to the public health authority as the recipient of the limited data set – neither disclosure requires an accounting. A disclosure to a business associate for the purpose of creating a limited data set is a health care operation, as defined by the Rule at 45 CFR 164.501. Disclosures for health care operations and disclosures made as a limited data set are both excepted from the accounting requirement at 45 CFR 164.528(a)(1)(i) and (viii), respectively.
May a covered entity use or disclose a patient’s entire medical record based on the patient’s signed Authorization?

Answer

Yes, as long as the Authorization describes, among other things, the information to be used or disclosed by the covered entity in a "specific and meaningful fashion," and is otherwise valid under the Privacy Rule. See 45 CFR 164.508(b)(1) and 164.508(c)(1)(i). An Authorization would be valid if it authorized the covered entity to use or disclose an "entire medical record" or "complete patient file." On the other hand, without further definition, an Authorization to use or disclose "all protected health information" might not be sufficiently specific, since protected health information encompasses a wider range of information than that which is typically understood to be included in the medical record, and individuals are less likely to understand the breadth of information that may be defined as "protected health information."

Last revised: March 26, 2007
Does the Privacy Rule permit a covered entity to use or disclose protected health information pursuant to an Authorization form that was prepared by a third party?

Answer

Yes. A covered entity is permitted to use or disclose protected health information pursuant to any Authorization that meets the Privacy Rule’s requirements at 45 CFR 164.508. The Privacy Rule requires that an Authorization contain certain core elements and statements, but does not specify who may draft an Authorization (i.e., it could be drafted by any entity) or dictate any particular format for an Authorization. Thus, a covered entity may disclose protected health information as specified in a valid Authorization that has been created by another covered entity or a third party, such as an insurance company or researcher.
May a valid Authorization list categories of persons who may use or disclose protected health information, without naming specific individuals or entities?

Answer

Yes. One Authorization form may be used to authorize uses and disclosures by classes or categories of persons or entities, without naming the particular persons or entities. See 45 CFR 164.508(c)(1)(ii). For example, it would be sufficient if an Authorization authorized disclosures by "any health plan, physician, health care professional, hospital, clinic, laboratory, pharmacy, medical facility, or other health care provider that has provided payment, treatment or services to me or on my behalf" or if an Authorization authorized disclosures by "all medical sources." A separate Authorization specifically naming each health care provider from whom protected health information may be sought is not required.

Similarly, the Rule permits the identification of classes of persons to whom the covered entity is authorized to make a disclosure. See 45 CFR 164.508(c)(1)(iii). Thus, a valid Authorization may authorize disclosures to a particular entity, particular person, or class of persons, such as "the employees of XYZ division of ABC insurance company."
Can an individual revoke his or her Authorization?

Answer

Yes. The Privacy Rule gives individuals the right to revoke, at any time, an Authorization they have given. The revocation must be in writing, and is not effective until the covered entity receives it. In addition, a written revocation is not effective with respect to actions a covered entity took in reliance on a valid Authorization, or where the Authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy or the policy itself.

The Privacy Rule requires that the Authorization must clearly state the individual’s right to revoke; and the process for revocation must either be set forth clearly on the Authorization itself, or if the covered entity creates the Authorization, and its Notice of Privacy Practices contains a clear description of the revocation process, the Authorization can refer to the Notice of Privacy Practices. Authorization forms created by or submitted through a third party should not imply that revocation is effective when the third party receives it, since the revocation is not effective until a covered entity which had previously been authorized to make the disclosure receives it.
Is a copy, facsimile, or electronically transmitted version of a signed Authorization valid under the Privacy Rule?

Answer

Yes. Under the Privacy Rule, a covered entity may use or disclose protected health information pursuant to a copy of a valid and signed Authorization, including a copy that is received by facsimile or electronically transmitted.

Last revised: April 03, 2007
Must an Authorization include an expiration date?

Answer

The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example, an Authorization may expire "one year from the date the Authorization is signed," "upon the minor's age of majority," or "upon termination of enrollment in the health plan." An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event. The fact that the expiration date on an Authorization may exceed a time period established by State law does not invalidate the Authorization under the Privacy Rule, but a more restrictive State law would control how long the Authorization is effective.

Last revised: March 26, 2007
May a covered entity disclose protected health information specified in an Authorization, even if that information was created after the Authorization was signed?

Answer

Yes, provided that the Authorization encompasses the category of information that was later created, and that the Authorization has not expired or been revoked by the individual. Unless otherwise expressly limited by the Authorization, a covered entity may use or disclose the protected health information identified on the Authorization regardless of when the information was created.

Last revised: March 26, 2007
Does the Privacy Rule require that an Authorization be notarized or include a witness signature?

Answer

The Privacy Rule does not require that a document be notarized or witnessed.

Last revised: March 26, 2007
Can an Authorization be used together with other written instructions from the intended recipient of the information?

Answer

A transmittal or cover letter can be used to narrow or provide specifics about a request for protected health information as described in an Authorization, but it cannot expand the scope of the Authorization. For example, if an individual has authorized the disclosure of "all medical records" to an insurance company, the insurance company could by cover letter narrow the request to the medical records for the last 12 months. The cover letter could also specify a particular employee or address for the "class of persons" designated in the Authorization to receive the information. By contrast, an insurance company could not by cover letter extend the expiration date of an Authorization, or expand the scope of information set forth in the Authorization.
Does the HIPAA Privacy Rule permit doctors, nurses, and other health care providers to share patient health information for treatment purposes without the patient’s authorization?

Answer

Yes. The Privacy Rule allows those doctors, nurses, hospitals, laboratory technicians, and other health care providers that are covered entities to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient’s authorization. This includes sharing the information to consult with other providers, including providers who are not covered entities, to treat a different patient, or to refer the patient. See 45 CFR 164.506.
Does the HIPAA Privacy Rule permit a doctor, laboratory, or other health care provider to share patient health information for treatment purposes by fax, e-mail, or over the phone?

**Answer**

Yes. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.

For example:

- A laboratory may fax, or communicate over the phone, a patient’s medical test results to a physician.
- A physician may mail or fax a copy of a patient’s medical record to a specialist who intends to treat the patient.
- A hospital may fax a patient’s health care instructions to a nursing home to which the patient is to be transferred.
- A doctor may discuss a patient’s condition over the phone with an emergency room physician who is providing the patient with emergency care.
- A doctor may orally discuss a patient’s treatment regimen with a nurse who will be involved in the patient’s care.
- A physician may consult with another physician by e-mail about a patient’s condition.
- A hospital may share an organ donor’s medical information with another hospital treating the organ recipient.

The Privacy Rule requires that covered health care providers apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. These safeguards may vary depending on the mode of communication used. For example, when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve a provider first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information. When discussing patient health information orally with another provider in proximity of others, a doctor may be able to reasonably safeguard the information by lowering his or her voice.
Does the HIPAA Privacy Rule permit hospitals and other health care facilities to inform visitors or callers about a patient's location in the facility and general condition?

Answer

Yes. Covered hospitals and other covered health care providers can use a facility directory to inform visitors or callers about a patient's location in the facility and general condition. The Privacy Rule permits a covered hospital or other covered health care provider to maintain in a directory certain information about patients – patient name, location in the facility, health condition expressed in general terms that does not communicate specific medical information about the individual, and religious affiliation. The patient must be informed about the information to be included in the directory, and to whom the information may be released, and must have the opportunity to restrict the information or to whom it is disclosed, or opt out of being included in the directory. The patient may be informed, and make his or her preferences known, orally or in writing. The facility may provide the appropriate directory information – except for religious affiliation – to anyone who asks for the patient by name. Religious affiliation may be disclosed to members of the clergy, who are given additional access to directory information under the Rule. (See other FAQs at this site by searching on the term “clergy”.)

Even when, due to emergency treatment circumstances or incapacity, the patient has not been provided an opportunity to express his or her preference about how, or if, the information may be disclosed, directory information about the patient may still be made available if doing so is in the individual’s best interest as determined in the professional judgment of the provider, and would not be inconsistent with any known preference previously expressed by the individual. In these cases, as soon as practicable, the covered health care provider must inform the patient about the directory and provide the patient an opportunity to express his or her preference about how, or if, the information may be disclosed. See 45 CFR 164.510(a).
Does the HIPAA Privacy Rule permit a hospital to inform callers or visitors of a patient’s location and general condition in the emergency room, even if the patient’s information would not normally be included in the main hospital directory of admitted patients?

Answer

Yes. The Privacy Rule permits covered entities to maintain more than one type of patient directory, and to maintain multiple versions of them, provided that the other requirements at 45 CFR 164.510(a) also are followed. For instance, emergency rooms that maintain directory information, even though separate from, or in a form different than, the hospital directory of admitted patients, may still disclose the information consistent with the requirements of the Privacy Rule. For further information about how this section of the Rule applies, see our other FAQs on this topic by searching on the term "directory."
Can the fact that a patient has been "treated and released," or that a patient has died, be released as part of the facility directory?

Answer

Yes. The fact that a patient has been "treated and released," or that a patient has died, may be released as part of the directory information about the patient's general condition and location in the facility, provided that the other requirements at 45 CFR 164.510(a) also are followed. For further information about how this section of the Rule applies, see our other FAQs on this topic by searching on the term "directory."

Last revised: April 03, 2007
Can the phone number of a patient's room be released as part of the facility directory?

Answer

Yes. The phone number of the patient's room in the facility may be released as part of the directory information about the patient's location in the facility, provided that the other requirements at 45 CFR 164.510(a) also are followed. For further information about how this section of the Rule applies, see our other FAQs on this topic by searching on the term "directory."

Last revised: April 03, 2007
May a hospital or other covered entity notify a patient's family member or other person that the patient is at their facility?

Answer

Yes. The HIPAA Privacy Rule, at 45 CFR 164.510(b), permits covered entities to notify, or assist in the notification of, family members, personal representatives, or other persons responsible for the care of the patient, of the patient's location, general condition, or death. Where the patient is present, or is otherwise available prior to the disclosure, and has capacity to make health care decisions, the covered entity may notify family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also use or disclose this information to notify the family and these other persons if it can reasonably infer from the circumstances, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may call a patient's wife to tell her that her husband was in a car accident and is being treated in the emergency room for minor injuries.

- A doctor may contact a pregnant patient's husband to let him know that his wife arrived at the hospital in labor and is about to give birth.

- A nurse may contact the patient's friend to let him know that his roommate broke his leg falling down the stairs, has had surgery, and is in recovery.

Even when the patient is not present or it is impracticable because of emergency or incapacity to ask the patient about notifying someone, a covered entity can still notify family and these other persons when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). For example, a doctor may, using such professional judgment, call the adult daughter of an incapacitated patient to inform her that her father suffered a stroke and is in the intensive care unit of a hospital.
Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?

Answer

Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for healthcare. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make healthcare decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient’s payment options with her adult daughter.
- A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient’s incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). Thus, for example:

- A surgeon may, if consistent with such professional judgment, inform a patient’s spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient’s progress and prognosis.
- A doctor may, if consistent with such professional judgment, discuss an incapacitated patient’s condition with a family member over the phone.

In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient’s best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.
When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative?

Answer

In general, and as explained below, the Privacy Rule permits a covered health care provider (covered provider), without the individual's written authorization, to disclose protected health information to a medical device company representative (medical device company) for the covered provider's own treatment, payment, or health care operation purposes (45 CFR 164.506(c)(1)), or for the treatment or payment purposes of a medical device company that is also a health care provider (45 CFR 164.506(c)(2), (3)). Additionally, the public health provisions of the Privacy Rule permit a covered provider to make disclosures, without an authorization, to a medical device company or other person that is subject to the jurisdiction of the Food and Drug Administration (FDA) for activities related to the quality, safety, or effectiveness of an FDA-regulated product or activity for which the person has responsibility. See 45 CFR 164.512(b)(1)(iii) and the frequently asked questions on public health disclosures for more information.

In certain situations, a covered health care provider may disclose protected health information to a medical device company without an individual's written authorization only if the medical device company is a health care provider as defined by the Rule. A medical device company meets the Privacy Rule's definition of "health care provider" if it furnishes, bills, or is paid for "health care" in the normal course of business. "Health care" under the Rule means care, services or supplies related to the health of an individual. Thus, a device manufacturer is a health care provider under the Privacy Rule if it needs protected health information to counsel a surgeon on or determine the appropriate size or type of prosthesis for the surgeon to use during a patient's surgery, or otherwise assists the doctor in adjusting a device for a particular patient. Similarly, when a device company needs protected health information to provide support and guidance to a patient, or to a doctor with respect to a particular patient, regarding the proper use or insertion of the device, it is providing "health care" and, therefore, is a health care provider when engaged in these services. See 65 FR 82569. By contrast, a medical device company is not providing "health care" if it simply sells its appropriately labeled products to another entity for that entity to use or dispense to individuals.

The following are some examples of circumstances in which a covered provider may share protected health information with a medical device company, without the individual’s authorization:

• A covered provider may disclose protected health information needed for an orthopaedic device manufacturer or its representative to determine and deliver the appropriate range of sizes of a prosthesis for the surgeon to use during a particular patient's surgery. (This would be a treatment disclosure to the device company as a health care provider. Exchanges of protected health information between health care providers for treatment of the individual are not subject to the minimum necessary

When may a covered health care provider disclose protected health information, without a... Page 2 of 2

standards. 45 CFR 164.502(b).

• The device manufacturer or its representative may be present in the operating room, as requested by the surgeon, to provide support and guidance regarding the appropriate use, implantation, calibration or adjustment of a medical device for that particular patient. (This would be treatment by the device company as a health care provider. As noted in the prior example, treatment disclosures between health care providers are not subject to the minimum necessary standards.)

• A covered provider may allow a representative of a medical device manufacturer to view protected health information, such as films or patient records, to provide consultation, advice or assistance where the provider, in her professional judgment, believes that this will assist with a particular patient’s treatment. (This would also be a treatment disclosure and minimum necessary would not apply.)

• A covered provider may share protected health information with a medical device company as necessary for the device company to receive payment for the health care it provides. (This would be a disclosure for payment of a health care provider and subject to minimum necessary standards.)

• A covered provider may disclose protected health information to a medical device manufacturer that is subject to FDA jurisdiction to report an adverse event, to track an FDA-regulated product, or other purposes related to the quality, safety, or effectiveness of the FDA-regulated product. (This would be a public health disclosure and subject to minimum necessary standards.)

A business associate agreement would not usually be required for the disclosures noted above. For example, a business associate agreement would not be needed for disclosures between health care providers for the treatment of the individual (45 CFR 164.502(e)(1)(ii)(A)). Likewise, a medical device company would not be a business associate of a covered provider with respect to public health disclosures to a device company that is subject to FDA jurisdiction or disclosures to a device company as a health care provider for that company’s payment purposes, as in neither case is the device company performing a function or activity on behalf of, nor providing a specified service to, the covered provider. See 45 CFR 160.103. In other circumstances, however, a business associate agreement may be required even if the disclosure were permitted without an authorization. For example, a business associate agreement would be required if a covered entity asked the medical device company to provide an estimate of the cost savings it might expect from the use of a particular medical device; and to do so, the device company needed access to the covered entity’s protected health information. In this case, the medical device company is performing a health care operations function (business planning and development) on behalf of the covered provider, which requires a business associate agreement even though the disclosure is permitted without an authorization.
May a doctor or hospital disclose protected health information to a person or entity that can assist in notifying a patient’s family member of the patient’s location and health condition?

Answer

Yes. The HIPAA Privacy Rule permits a covered doctor or hospital to disclose protected health information to a person or entity that will assist in notifying a patient’s family member of the patient’s location, general condition, or death. See 45 CFR 164.510(b)(1)(ii). The patient’s written authorization is not required to make disclosures to notify, identify, or locate the patient’s family members, his or her personal representatives, or other persons responsible for the patient’s care. Rather, where the patient is present, or is otherwise available prior to the disclosure, and has capacity to make health care decisions, the covered entity may disclose protected health information for notification purposes if the patient agrees or, when given the opportunity, does not object. The covered entity may also make the disclosure if it can reasonably infer from the circumstances, based on professional judgment, that the patient does not object. See 45 CFR 164.510(b)(2).

Even when the patient is not present or it is impracticable because of emergency or incapacity to ask the patient about notifying someone, a covered entity can still disclose a patient’s location, general condition, or death for notification purposes when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b)(3).

Under these circumstances, for example:

- A doctor may share information about a patient’s condition with the American Red Cross for the Red Cross to provide emergency communications services for members of the U.S. military, such as notifying service members of family illness or death, including verifying such illnesses for emergency leave requests.

- A hospital may ask police to help locate and communicate with the family of an individual killed or injured in an accident.

- A hospital may contact a patient’s employer for information to assist in locating the patient’s spouse so that he/she may be notified about the hospitalization of the patient.
Must all small health plans comply with the Privacy Rule?

Answer

No. Certain plans are specifically excluded from having to comply with the HIPAA Administrative Simplification requirements, including the Privacy Rule. See 45 CFR 160.103. An employee welfare benefit plan that has less than 50 participants and is administered by the employer that establishes and maintains the plan is not a HIPAA covered entity. These plans, therefore, are not subject to the Privacy Rule. For additional information regarding compliance with the Privacy Rule, see the Department of Health and Human Services Office for Civil Rights website at: http://www.hhs.gov/ocr/hipaa.
I’m an employer that offers a fully insured group health plan for my employees. Is the fully insured group health plan subject to all of the Privacy Rule provisions?

Answer

The Privacy Rule recognizes that certain fully insured group health plans may not need to satisfy all of the requirements of the Privacy Rule since these responsibilities will be carried out by the health insurance issuer or HMO with which the group health plan has contracted for coverage of its members. In particular, a fully insured group health plan that does not create or receive protected health information other than summary health information (see definition at 45 CFR 164.504(a)) and enrollment or disenrollment information is not required to have or provide a notice of privacy practices. See 45 CFR 164.520(a)(2). Moreover, these group health plans are exempt from most of the administrative responsibilities under the Privacy Rule. See 45 CFR 164.530(k). These health plans are still required, however, to refrain from intimidating or retaliatory acts (45 CFR 164.530(g)), and from requiring an individual to waive their privacy rights (45 CFR 164.530(h)). The documentation requirements at 45 CFR 164.530(j) apply to these group health plans only to the extent of amendments, if any, made to the plan documents for the sharing of information with the plan sponsor under 45 CFR 164.504(f). Additional information about the Privacy Rule, including guidance and technical assistance materials is available through the Department of Health and Human Services Office for Civil Rights website at: http://www.hhs.gov/ocr/hipaa.

Last revised: March 26, 2007
Does the April 14, 2004, deadline for small health plan compliance with the Privacy Rule impose any new or additional requirements on health plans that are already subject to compliance with the Privacy Rule?

Answer

No.

Last revised: April 03, 2007
When a covered entity, such as a doctor, uses a certified Telecommunications Relay Service to contact patients with hearing or speech impairments, is the Relay Service a business associate of the doctor?

Answer

Under the Privacy Rule, a covered entity such as a doctor can contact a patient using a Telecommunications Relay Service (TRS), without the need for a business associate contract with the TRS. The sharing of protected health information between a covered health care provider and a patient through the TRS is permitted by the Privacy Rule under 45 C.F.R. 164.510(b), and a business associate contract is not required in these circumstances.

By way of background, the TRS enables telephone communication for people with hearing or speech impairments by using a communications assistant (CA) who transliterates conversations. The TRS CA relays information, which may include protected health information, between a text telephone (also known as "TTY") user and another person communicating via voice. The CA must communicate what is said by the parties without alteration. The Federal Communications Commission (FCC), pursuant to the Americans with Disabilities Act (ADA), certifies all State TRS programs, which in turn contract with one or more TRS providers. All TRS providers must comply with standards for operators established by the FCC pursuant to Title IV of the ADA, including protecting the privacy of all relayed communications. The TRS is a public service that is available without cost to all persons and businesses, none of whom need to employ, contract with or otherwise establish business relationships with the TRS. Thus, when performing these services, the TRS is not acting for or on behalf of the covered entity and is not the covered entity's business associate.

As permitted by 45 C.F.R. 164.510(b), protected health information can be shared during a telephone communication using the TRS because the individual will have an opportunity to agree or object to disclosures of protected health information to the CA. The following typical scenarios describe how this opportunity can be provided in the course of, or prior to, using the TRS:

- Where the individual initiates the call through the TRS, it is reasonable for a covered health care provider to infer from these circumstances that the individual has identified the CA as involved in the individual’s care, and that the individual does not object to the disclosure. See 45 C.F.R. 164.510(b)(2)(iii).

- Where the need for use of the TRS becomes apparent prior to a call being placed, such as when, during an office visit, the individual gives the health care provider his or her TTY number, the opportunity to agree or object to the TRS can be provided at that time. See 45 C.F.R. 164.510(b)(2).

- Even where the covered health care provider initiates a call using the TRS without the individual’s prior agreement, the individual will have an opportunity to agree or object at the outset of the call. Typically, the CA will begin the call by identifying the service to the party called, and if that party is unfamiliar with the TRS, the CA will
briefly explain how the service operates. This initial contact by the CA provides the individual with the opportunity to agree to the disclosure by proceeding with the call using the TRS, or to object by terminating the call. See 45 C.F.R. 164.510(b)(2)(i)-(ii).

Last revised: March 26, 2007
When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?

Answer

The Privacy Rule is balanced to protect an individual’s privacy while allowing important law enforcement functions to continue. The Rule permits covered entities to disclose protected health information (PHI) to law enforcement officials, without the individual’s written authorization, under specific circumstances summarized below. For a complete understanding of the conditions and requirements for these disclosures, please review the exact regulatory text at the citations provided. Disclosures for law enforcement purposes are permitted as follows:

- To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena. The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual’s private information (45 CFR 164.512(f)(1)(ii) (A)-(B)).

- To respond to an administrative request, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512(f)(1)(ii)(C)).

- To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures of PHI to 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, and a description of distinguishing physical characteristics. Other information related to the individual’s DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request (45 CFR 164.512(f)(2)).

This same limited information may be reported to law enforcement:

- About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity’s workforce (45 CFR 164.502(j)(2));

- To identify or apprehend an individual who has admitted participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individual’s request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512(j)(1)(ii)(A), (j)(2)-(3)).
• To respond to a request for PHI about a victim of a crime, and the victim agrees. If, because of an emergency or the person’s incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512(f)(3)).

Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, other provisions of the Rule apply:

- Child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512(b)(1)(ii)).

- Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such reports (45 CFR 164.512(c)):
  - If the individual agrees;
  - If the report is required by law; or
  - If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (see 45 CFR 164.512(c) (1)(iii)(B)).

- Notice to the individual of the report may be required (see 45 CFR 164.512 (c)(2)).

• To report PHI to law enforcement when required by law to do so (45 CFR 164.512(f)(1)(i)). For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.

• To alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct (45 CFR 164.512(f)(4)).

- Information about a decedent may also be shared with medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties (45 CFR 164.512(g)(1)).

• To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity’s premises (45 CFR 164.512(f)(5)).

• When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and location of the perpetrator of the crime (45 CFR 164.512(f)(6)). This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect, or domestic violence for when reports to law enforcement are required.
When does the Privacy Rule allow covered entities to disclose protected health information?

Enforcement are allowed under 45 CFR 164.512(c).

- When consistent with applicable law and ethical standards:
  - To a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public (45 CFR 164.512(j)(1)(i)); or
  - To identify or apprehend an individual who appears to have escaped from lawful custody (45 CFR 164.512(j)(1)(ii)(B)).

- For certain other specialized governmental law enforcement purposes, such as:
  - To federal officials authorized to conduct intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));
  - To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the health and safety of the individual, other inmates, officers or employees of or others at a correctional institution or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

Except when required by law, the disclosures to law enforcement summarized above are subject to a minimum necessary determination by the covered entity (45 CFR 164.502(b), 164.514(d)). When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)). Moreover, if the law enforcement official making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)).
State public records laws, also known as open records or freedom of information laws, all provide for certain public access to government records. How does the HIPAA Privacy Rule relate to these state laws?

**Answer**

If a state agency is not a "covered entity", as that term is defined at 45 CFR 160.103, it is not required to comply with the HIPAA Privacy Rule and, thus, any disclosure of information by the state agency pursuant to its state public records law would not be subject to the Privacy Rule.

If a state agency is a covered entity, however, the Privacy Rule applies to its disclosures of protected health information. The Privacy Rule permits a covered entity to use and disclose protected health information as required by other law, including state law. See 45 CFR 164.512(a). Thus, where a state public records law mandates that a covered entity disclose protected health information, the covered entity is permitted by the Privacy Rule to make the disclosure, provided the disclosure complies with and is limited to the relevant requirements of the public records law.

However, where a state public records law only permits, and does not mandate, the disclosure of protected health information, or where exceptions or other qualifications apply to exempt the protected health information from the state law’s disclosure requirement, such disclosures are not “required by law” and thus, would not fall within § 164.512(a) of the Privacy Rule. For example, if a state public records law includes an exemption that affords a state agency discretion not to disclose medical or other information where such disclosure would constitute a clearly unwarranted invasion of personal privacy, the disclosure of such records is not required by the public records law, and therefore is not permissible under § 164.512(a). In such cases, a covered entity only would be able to make the disclosure if permitted by another provision of the Privacy Rule.

As an example of how the Privacy Rule would apply in the case where an exemption exists in a freedom of information law, see the December 2000 Privacy Rule preamble discussion regarding the relationship of the Privacy Rule with the federal Freedom of Information Act (64 FR 82482).
May a covered entity disclose protected health information in response to a court order?

Yes. A covered entity may disclose protected health information to comply with a court order, including an order of an administrative tribunal. Such disclosures must be limited to the protected health information expressly authorized by the order. See 45 CFR 164.512(e)(1)(i).

Last revised: April 03, 2007
May a covered entity use or disclose protected health information for litigation?

Answer

A covered entity may use or disclose protected health information as permitted or required by the Privacy Rule, see 45 CFR 164.502(a); and, subject to certain conditions the Rule typically permits uses and disclosures for litigation, whether for judicial or administrative proceedings, under particular provisions for judicial and administrative proceedings set forth at 45 CFR 164.512(e), or as part of the covered entity's health care operations, 45 CFR 164.506(a). Depending on the context, a covered entity's use or disclosure of protected health information in the course of litigation also may be permitted under a number of other provisions of the Rule, including uses or disclosures that are required by law (as when the court has ordered certain disclosures), that are for a proceeding before a health oversight agency (as in a contested licensing revocation), that are for payment purposes (as in a collection action on an unpaid claim), or that are with the individual's written authorization.

Where a covered entity is a party to a legal proceeding, such as a plaintiff or defendant, the covered entity may use or disclose protected health information for purposes of the litigation as part of its health care operations. The definition of “health care operations” at 45 CFR 164.501 includes a covered entity's activities of conducting or arranging for legal services to the extent such activities are related to the covered entity's covered functions (i.e., those functions that make the entity a health plan, health care provider, or health care clearinghouse), including legal services related to an entity's treatment or payment functions. Thus, for example, a covered entity that is a defendant in a malpractice action or a plaintiff in a suit to obtain payment may use or disclose protected health information for such litigation as part of its health care operations. The covered entity, however, must make reasonable efforts to limit such uses and disclosures to the minimum necessary to accomplish the intended purpose. See 45 CFR 164.502(b), 164.514(d).

Where the covered entity is not a party to the proceeding, the covered entity may disclose protected health information for the litigation in response to a court order, subpoena, discovery request, or other lawful process, provided the applicable requirements of 45 CFR 164.512(e) for disclosures for judicial and administrative proceedings are met.
May a covered entity that is a plaintiff or defendant in a legal proceeding use or disclose protected health information for the litigation?

Answer

Yes. Where a covered entity is a party to a legal proceeding, such as a plaintiff or defendant, the covered entity may use or disclose protected health information for purposes of the litigation as part of its health care operations. The definition of “health care operations” at 45 CFR 164.501 includes a covered entity’s activities of conducting or arranging for legal services to the extent such activities are related to the covered entity’s covered functions (i.e., those functions that make the entity a health plan, health care provider, or health care clearinghouse). Thus, for example, a covered entity that is a defendant in a malpractice action, or a plaintiff in a suit to obtain payment, may use or disclose protected health information for such litigation as part of its health care operations.

The covered entity, however, must make reasonable efforts to limit such uses and disclosures to the minimum necessary to accomplish the intended purpose. See 45 CFR 164.502(b), 164.514(d). In most cases, the covered entity will share protected health information for litigation purposes with its lawyer, who is either a workforce member or a business associate. In these cases, the Privacy Rule permits a covered entity to reasonably rely on the representations of a lawyer who is a business associate or workforce member that the information requested is the minimum necessary for the stated purpose. See 45 CFR 164.514(d)(3)(iii)(C). A covered entity’s minimum necessary policies and procedures may provide for such reasonable reliance on the lawyer’s requests for protected health information needed in the course of providing legal services to the covered entity.

In disclosing protected health information for litigation purposes, the lawyer who is a workforce member of the covered entity must make reasonable efforts to limit the protected health information disclosed to the minimum necessary for the purpose of the disclosure. Similarly, a lawyer who is a business associate must apply the minimum necessary standard to its disclosures, as the business associate contract may not authorize the business associate to further use or disclose protected health information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. Depending on the circumstances, this could involve de-identifying the information or stripping direct identifiers from the information to protect the privacy of individuals, and may in some cases limit disclosures more significantly than would be required to meet a “relevance” standard. Further, whether as workforce members or business associates, lawyers may consider availing themselves of the protections routinely afforded to similarly confidential information within the litigation forum, such as protective orders on the use of the information in public portions of the proceedings.
What “satisfactory assurances” must a covered entity that is not a party to the litigation receive before it may respond to a subpoena without a court order?

Answer

Under 45 CFR 164.512(e)(1)(ii) of the Privacy Rule, a covered entity that is not a party to the litigation may disclose protected health information in response to a subpoena, discovery request, or other lawful process if the covered entity receives certain satisfactory assurances from the party seeking the information. Specifically, the covered entity must receive a written statement and accompanying documentation that the requestor has made reasonable efforts either (1) to ensure that the individual(s) who are the subject of the information have been given sufficient notice of the request, or (2) to secure a qualified protective order. (Alternatively, the covered entity may make such disclosures if it itself makes reasonable efforts to notify the individual(s) or seek a qualified protective order.) If the conditions above have been met, a court order is not required to make the disclosure.

For notice to the individual(s), the written statement and accompanying documentation must demonstrate that the requestor has made a good faith attempt to provide written notice to the individual; and that the notice included sufficient information about the litigation to permit the individual to raise an objection with the court, the time for the individual to raise an objection has elapsed, and no objections were filed or all objections filed were resolved and the request is consistent with the resolution. Such statements and documentation may include, for example, a copy of the notice mailed to the individual that includes instructions for raising an objection with the court and the deadline for doing so, and a written statement or other documentation demonstrating that no objections were raised or all objections raised were resolved and the request is consistent with the resolution. To the extent that the subpoena or other request itself demonstrates the above elements, no additional documentation is required.

For a qualified protective order, the written statement and accompanying documentation must demonstrate that the parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or the party seeking the protected health information has requested a qualified protective order from the court or administrative tribunal. See the definition of “qualified protective order” at 45 CFR 164.512(e)(1)(v). Such statements and documentation may include, for example, a copy of the qualified protective order that the parties have agreed to and documentation or a statement that the order was presented to the court, or a copy of the motion to the court requesting a qualified protective order.
For disclosures for judicial and administrative proceedings, can notice be provided to the individual's lawyer instead of the individual?

Answer

Yes. A covered entity that is not a party to litigation must obtain or receive the satisfactory assurances required by 45 CFR 164.512(e) before making a disclosure for a judicial or administrative proceeding. Where the satisfactory assurances are in the form of notice to the individual, a written statement and accompanying documentation of notice to the individual’s lawyer is considered to be notice to the individual and, thus, suffices, provided the documentation otherwise meets the requirements of 45 CFR 164.512(e)(1)(iii). Specifically, the written statement and accompanying documentation must demonstrate that the notice included sufficient information about the litigation to permit the individual to raise an objection to the court; and that the time for the individual to raise objections has elapsed, with no objections having been filed, or all filed objections having been resolved.
For disclosures for judicial and administrative proceedings, when is a copy of the subpoena itself sufficient satisfactory assurance of notice to the individual?

Answer

A copy of the subpoena (or other request pursuant to lawful process) is sufficient when, on its face, it meets the requirements of 45 CFR 164.512(e)(1)(iii), such as by demonstrating that the individual whose protected health information is requested is a party to the litigation, notice of the request has been provided to the individual or his or her attorney, and the time for the individual to raise objections has elapsed and no objections were filed or all objections filed have been resolved. When the above requirements are evident on the face of the subpoena (or other request), no additional documentation is required.

Last revised: March 26, 2007
In providing legal services to a covered entity, must a lawyer who is a business associate require that those persons to whom it discloses protected health information agree to abide by the privacy restrictions and conditions that apply to the lawyer?

Answer

It depends on who the recipient is. The business associate agreement between the covered entity and the lawyer-business associate must provide that the lawyer will ensure that any agents, including subcontractors, to whom it provides protected health information agree to the same restrictions and conditions that apply to the business associate with respect to the information. See 45 CFR 164.504(e)(2)(ii)(D). Thus, if a lawyer-business associate enlists the services of a person or entity in furtherance of the lawyer’s legal services to a covered entity, and the lawyer must provide protected health information to the person or entity for such purpose, the lawyer’s business associate contract with the covered entity requires that the lawyer ensure that these persons agree to the same restrictions and conditions with respect to the protected health information they receive that apply to the lawyer as a business associate. For example, pursuant to its business associate contract, a lawyer must ensure that other legal counsel, jury experts, document or file managers, investigators, litigation support personnel, or others hired by the lawyer to assist the lawyer in providing legal services to the covered entity, will also safeguard the privacy of the protected health information the lawyer receives to perform its duties. Conversely, a lawyer-business associate need not ensure that opposing counsel, fact witnesses, or other persons who do not perform functions or services that assist the lawyer in performing its services to the client, agree to the business associate restrictions and conditions, even though the lawyer may have to disclose protected health information to these third parties.
When must a covered entity account for disclosures of protected health information made during the course of litigation?

Answer

Individuals have a right to receive, upon request, an accounting of disclosures of protected health information made by a covered entity (or its business associate), with certain exceptions. These exceptions, or instances where a covered entity is not required to account for disclosures, include disclosures for treatment, payment, or health care operations and disclosures authorized by the Individual. See 45 CFR 164.528. Disclosures that are subject to the accounting for disclosures requirement include disclosures made by a covered entity that is not a party to the litigation or proceeding and that are made: (1) as required by law (under §§ 164.512(a) and (e) (1)(i)); (2) for a proceeding before a health oversight agency (under § 164.512(d)); or (3) in response to a subpoena, discovery request, or other lawful process (under § 164.512(e)). Conversely, covered entities need not account for disclosures of protected health information for litigation that are made with the individual's authorization or, in cases where the covered entity is a party to the litigation, when such disclosures are part of the covered entity's health care operations.

In many cases, covered entities share protected health information for litigation purposes with a lawyer who is a business associate of the covered entity. These disclosures by a covered entity to its lawyer-business associate are not themselves subject to the accounting. However, if (as described above) the lawyer makes disclosures that are subject to the accounting requirement, the business associate agreement required by the Privacy Rule must provide that the lawyer-business associate must make information about these disclosures available to the covered entity, so that the covered entity can fulfill its obligation to provide an accounting to the individual. Alternatively, the covered entity and the lawyer can agree through the business associate contract that the lawyer will provide the accounting to individuals who request one.
May a covered entity that is not a party to a legal proceeding disclose protected health information in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order?

Answer

Yes, if certain conditions are met. A covered entity that is not a party to litigation, such as where the covered entity is neither a plaintiff nor a defendant, may disclose protected health information in response to a subpoena, discovery request, or other lawful process, that is not accompanied by a court order, provided that the covered entity:

- Receives a written statement and accompanying documentation from the party seeking the information that reasonable efforts have been made either (1) to ensure that the individual(s) who are the subject of the information have been notified of the request, or (2) to secure a qualified protective order for the information; or

- Itself makes reasonable efforts either (1) to provide notice to the individual(s) that meets the same requirements as set forth below for sufficient notice by the party making the request, or (2) to seek a qualified protective order as defined below. See 45 CFR 164.512(e).

The covered entity must make reasonable efforts to limit the protected health information used or disclosed to the minimum necessary to respond to the request. See 45 CFR 164.502(b) and 164.514(d).

The requirement to provide sufficient notice to the individual(s) is met when a party provides a written statement and accompanying documentation that demonstrates:

- A good faith attempt was made to notify the individual (or if the individual’s location is unknown, to mail a notice to the individual’s last known address);

- The notice included sufficient detail to permit the individual to raise an objection with the court or administrative tribunal; and

- The time for the individual to raise objections under the rules of the court or tribunal has lapsed and no objections were filed or all objections filed by the individual have been resolved by the court and the disclosures being sought are consistent with the resolution.

A qualified protective order is an order of a court or administrative tribunal or a stipulation by the parties that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and requires the return to the covered entity or destruction of the protected health information (including any copies) at...
the end of the litigation or proceeding. The party requesting the information must provide a written statement and accompanying documentation that demonstrates:

- The parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or

- The party seeking the protected health information has requested a qualified protective order from the court or administrative tribunal.
May a health plan disclose protected health information to a State child support enforcement (IV-D) agency in response to a National Medical Support Notice?

Answer

The Privacy Rule permits a health plan to respond to a request for information by a IV-D agency pursuant to a National Medical Support Notice (NMSN), as described below.

The Privacy Rule at 45 CFR 164.512(f) permits a covered entity to disclose protected health information to a "law enforcement official" for law enforcement purposes in compliance with court orders, grand jury subpoenas, or certain written administrative requests. 45 CFR 164.512(f)(1)(ii). As defined in 45 CFR 164.501, a "law enforcement official" means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law or to prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. An employee of a IV-D agency, including a contract employee, who is empowered by state or federal law to enforce a medical child support order, meets this definition of a law enforcement official.

The NMSN, a nationally uniform form which is sent by the IV-D agency to the employer and health plan for completion, constitutes a written administrative request by a law enforcement official. As such, the Privacy Rule allows a health plan to disclose protected health information in response to the NMSN, provided it includes or is accompanied by written assurances by the law enforcement official that (1) the information sought is material and relevant to a legitimate law enforcement inquiry; (2) the request is specific and limited in scope; and (3) de-identified information cannot reasonably be used. 45 CFR 164.512(f)(1)(ii)(C).

The Privacy Rule requires the covered entity to verify that these three conditions are met, as well as the identity and authority of the public official making the request, unless already known to the covered entity. The covered entity must also limit the disclosures to the minimum necessary for the purpose. To meet these requirements, the covered entity may reasonably rely on the following:

- the NMSN, or a separate written statement that, on its face, demonstrates that the three assurances required for these disclosures have been met. 45 CFR 164.514(h)(2)(i)(A).
- the NMSN is sufficient to verify the identity and legal authority of the public official requesting the protected health information. 45 CFR 164.514(h)(2)(ii) and (iii).
- the NMSN is sufficient as a request from a public official for the minimum information needed to meet the law enforcement purpose of the request. 45 CFR 164.514(d)(3)(iii)(A).
Must a covered health care provider obtain an individual’s authorization to use or disclose protected health information to an interpreter?

Answer

No, when a covered health care provider uses an interpreter to communicate with an individual, the individual’s authorization is not required when the provider meets the conditions below. Covered entities may use and disclose protected health information for treatment, payment and health care operations without an individual’s authorization, 45 CFR 164.506(c). A covered health care provider might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the covered entity as defined at 45 CFR 164.501.

When using interpreter services, a covered entity may use and disclose protected health information regarding an individual without an individual’s authorization as a health care operation, in accordance with the Privacy Rule, in the following ways:

- When the interpreter is a member of the covered entity’s workforce (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer) as defined at 45 CFR 160.103;

- When a covered entity engages the services of a person or entity, who is not a workforce member, to perform interpreter services on its behalf, as a business associate, as defined at 45 CFR 160.103. A covered entity may disclose protected health information as necessary for the business associate to provide interpreter services on the covered entity’s behalf, subject to certain written satisfactory assurances set forth in 45 CFR 164.504(e). For instance, many providers -- including those that are recipients of federal financial assistance and are required under Title VI of the Civil Rights Act of 1964 to take reasonable steps to provide meaningful access to persons with limited English proficiency -- will have contractual arrangements with private commercial companies, community-based organizations, or telephone interpreter service lines to provide such language services. If a covered entity has an ongoing contractual relationship with an interpreter service, that service arrangement should comply with the Privacy Rule business associate agreement requirements.

In addition, a covered health care provider may, without the individual’s authorization, use or disclose protected health information to the patient’s family member, close friend, or any other person identified by the individual as his or her interpreter for a particular healthcare encounter. In these situations, that interpreter is not a business associate of the health care provider. As with other disclosures to family members, friends or other persons identified by an individual as involved in his or her care, when the individual is present, the covered entity may obtain the
Must a covered health care provider obtain an individual’s authorization to use or disclose protected health information? Yes, except when the individual agrees or reasonably infers, based on the exercise of professional judgment, that the individual does not object to the disclosure of protected health information. 45 CFR 164.510(b)(2). For example, if a covered health care provider encounters a patient who speaks a language for which the provider has no employee, volunteer member of the workforce or contractor who can competently interpret, but then is able to identify a telephone interpreter service to communicate with the patient, the provider may contact the telephone interpreter service and identify the language used by the patient, so that the interpreter may explain to the patient that the interpreter is available to assist the patient in communicating with the provider. If the provider reasonably concludes that the patient has chosen to be assisted by the interpreter, and, by the patient’s willingness to continue the health care encounter using the interpreter, reasonably infers that the individual does not object to the disclosure, protected health information may be disclosed in accordance with 45 CFR 164.510(b) without a business associate contract.

Organizations that are subject to both HIPAA and Title VI must comply with the requirements of both laws, though not all HIPAA covered entities are recipients of federal financial assistance and thus, required to comply with Title VI; and not all recipients of federal financial assistance are also HIPAA covered entities, subject to the Privacy Rule. For information about the obligation of recipients of federal financial assistance to take reasonable steps to provide meaningful access to persons who are limited English proficient, see Guidance to Federal Financial Assistance Recipients Regarding Title VI Prohibition Against National Origin Discrimination Affecting Limited English Proficient Persons available at http://www.hhs.gov/ocr/lep/. This guidance includes information for recipients of federal financial assistance about important considerations for determining the competency of interpreters, such as their understanding of applicable confidentiality requirements, that should be taken into account when using interpreters arranged by the provider or when individuals elect to use friends, family or others as interpreters.

HIPAA covered entities may also be required to comply with the Americans with Disabilities Act and/or Section 504 of the Rehabilitation Act of 1973, both of which have requirements for the provision of sign language and oral interpreters for people who are deaf or hard of hearing. The use of communications assistants as part of a Telecommunications Relay Service (TRS) was the subject of a previous FAQ available at http://www.hhs.gov/ocr/hipaa (click on Your Frequently Asked Questions About Privacy, and then search on “TRS”).

Last revised: April 03, 2007
May a covered entity disclose protected health information to a Protection and Advocacy system where the disclosure is required by law?

Answer

Yes. The Privacy Rule permits a covered entity to disclose protected health information (PHI) without the authorization of the individual to a state-designated Protection and Advocacy (P&A) system to the extent that such disclosure is required by law and the disclosure complies with the requirements of that law. 45 CFR 164.512(a). The Developmental Disabilities Assistance and Bill of Rights Act (DD Act) provides for each state to designate a public or private entity as the Protection and Advocacy system to protect and advocate for the rights of individuals with developmental disabilities, including investigating incidents of abuse or neglect. The P&A designated pursuant to the DD Act is also the Protection and Advocacy system for purposes of the Protection and Advocacy for Individuals with Mental Illness Act (PAIMI Act) and is empowered to protect and advocate for the rights of individuals with mental illness. These statutes and their implementing regulations require that access to records be provided to P&As under certain circumstances. See the DD Act at 42 USCA 15043(a)(2)(I) and (J) and the PAIMI Act at 42 USCA 10805(a)(4), and their implementing regulations at 45 CFR 1386.22 and 42 CFR 51.41, respectively. Thus, a covered entity may disclose PHI as required by the DD and PAIMI Acts to P&As requesting access to such records in carrying out their protection and advocacy functions under these Acts. Similarly, covered entities may disclose PHI to P&As where another federal, state or other law mandates such disclosures, consistent with the requirements in that law. Where disclosures are required by law, the Privacy Rule’s minimum necessary standard does not apply, since the law requiring the disclosure will establish the limits on what should be disclosed. Moreover, with respect to required by law disclosures, a covered entity cannot use the Privacy Rule as a reason not to comply with its other legal obligations.

Section 164.512(a)(2) provides that in making a “required by law” disclosure about adult abuse, neglect or domestic violence (section 164.512(c)), for judicial or administrative proceedings (section 164.512(e)), or for law enforcement purposes (section 164.512(f)), covered entities must also comply with any additional privacy requirements in these provisions that apply. However, none of the additional procedural protections in sections 164.512(c), (e) and (f) apply to the type of “required by law” disclosures to P&As under the provisions of the DD and PAIMI Acts discussed here.

Last revised: March 26, 2007
Can a group health plan, or health insurance issuer with respect to a group health plan, disclose to the plan sponsor the protected health information (PHI) required by the Centers for Medicare and Medicaid Services (CMS) for the retiree drug subsidy, without obtaining the individual’s authorization?

Answer

Yes, when the conditions set forth in 45 CFR 164.504(f) of the HIPAA Privacy Rule have been met. Specifically, 45 CFR 164.504(f)(3)(i) allows a group health plan or a health insurance issuer with respect to the group health plan – or its business associate – to disclose PHI to a plan sponsor to carry out plan administration functions as long as it meets the requirements of 45 CFR 164.504(f)(2). As such, where the plan sponsor is carrying out the plan administration function of submitting to CMS the PHI required by 42 CFR 423.884 for the retiree drug subsidy, 45 CFR 164.504(f)(2) sets forth how the group health plan’s plan documents are to be amended to allow the group health plan to permit its health insurance issuer (or business associate, such as a third party administrator) to disclose PHI, without the individual’s authorization, to the plan sponsor of the group health plan. As with other disclosures for plan administration functions, the PHI disclosed must be limited to the minimum necessary to fulfill the requirements of 42 CFR 423.884.
Can health care information be shared in a severe disaster?

Answer

Providers and health plans covered by the HIPAA Privacy Rule can share patient information in all of the following ways:

TREATMENT: Health care providers can share patient information as necessary to provide treatment.

Treatment includes:

- sharing information with other providers (including hospitals and clinics),
- referring patients for treatment (including linking patients with available providers in areas where the patients have relocated), and
- coordinating patient care with others (such as emergency relief workers or others that can help in finding patients appropriate health services).

Providers can also share patient information to the extent necessary to seek payment for these health care services.

NOTIFICATION: Health care providers can share patient information as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care of the individual's location, general condition, or death.

The health care provider should get verbal permission from individuals, when possible; but if the individual is incapacitated or not available, providers may share information for these purposes if, in their professional judgement, doing so is in the patient's best interest.

- Thus, when necessary, the hospital may notify the police, the press, or the public at large to the extent necessary to help locate, identify, or otherwise notify family members and others as to the location and general condition of their loved ones.
- In addition, when a health care provider is sharing information with disaster relief organizations that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, it is unnecessary to obtain a patient's permission to share the information if doing so would interfere with the organization's ability to respond to the emergency.

IMMEDIATE DANGER: Providers can share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public -- consistent with applicable law and the provider's standards of ethical conduct.

FACILITY DIRECTORY: Health care facilities maintaining a directory of patients can tell people who call or ask about individuals whether the individual is at the facility, their location in the facility, and general condition.
Of course, the HIPAA Privacy Rule does not apply to disclosures if they are not made by entities covered by the Privacy Rule. Thus, for instance, the HIPAA Privacy Rule does not restrict the American Red Cross from sharing patient information.

Last revised: March 26, 2007
May a Medicaid State agency and a Medicare Advantage plan share protected health information to identify dually eligible enrollees?

Answer

Yes. The HIPAA Privacy Rule permits a covered entity to disclose protected health information (PHI) both for its own payment purposes, as well as for the payment purposes of another covered entity that receives the information. See 45 CFR 164.506 (c)(3). The Privacy Rule defines “payment” to include activities to determine eligibility or coverage of enrollees. See the definition of “payment” at 45 CFR 164.501, paragraph (2)(i). Thus, a Medicaid State agency and a Medicare Advantage plan may disclose to each other PHI about their enrollees to identify those enrollees that are dually eligible under both plans. Such disclosures must comport with the Privacy Rule’s minimum necessary standard, where applicable. See 45 CFR 164.502(b), 164.514(d).

In general, an electronic inquiry and response from one health plan to another to obtain information regarding the eligibility of an enrollee to receive health care must be done using the HIPAA standard transaction for eligibility (X12N 270/271 transaction). Where the disclosures between the State Medicaid agency and the Medicare Advantage plan are conducted using the standard, the Privacy Rule’s minimum necessary requirements do not apply to the disclosures of the data elements required or situationally required by the standard transaction. In contrast, where the disclosures are made outside of a standard transaction, both the Medicare Advantage plan in its request for PHI, as well as the State Medicaid agency in its response, must make reasonable efforts to limit the PHI requested and disclosed to the minimum necessary PHI for the purpose of identifying dually eligible enrollees. Because the Medicare Advantage plan must limit its request to the minimum necessary PHI to identify dually eligible enrollees, the State Medicaid agency may rely, if reasonable, on that request for PHI as satisfying the minimum necessary requirement for these purposes. See 45 CFR 164.514(d)(3)(iii).
Is a health plan required to periodically notify enrollees about the availability, and how to obtain a copy, of its Notice of Privacy Practices?

Answer

Yes. The Privacy Rule requires a health plan to remind enrollees of the availability of its Notice of Privacy Practices, as well as how to obtain a copy, no less frequently than once every 3 years. See 45 CFR 164.520(c)(1)(ii).

Health plans may satisfy this requirement in a number of ways, including by:

- Sending a copy of their Notice of Privacy Practices.
- Mailing only a reminder concerning the availability of the Notice of Privacy Practices and information on how to obtain a copy.
- Including in a plan-produced newsletter or other publication information about the availability of the Notice of Privacy Practices and how to obtain a copy.

Health plans already may have satisfied the reminder requirement in a number of ways. For instance, a health plan may have adopted the practice of sending its Notice of Privacy Practices to subscribers and enrollees annually. Or, a health plan may have substantially amended its Notice of Privacy Practices recently, and thus, sent the revised Notice to its subscribers and enrollees as required by the Privacy Rule. See 45 CFR 164.520(c)(1)(i)(C). Moreover, a plan may have included information regarding the availability of its Notice of Privacy Practices in annual communications sent to subscribers and enrollees of the plan.

A health plan can satisfy the requirement by providing the reminder notice to the named insured of a policy under which coverage is provided to that named insured and one or more dependents. See 45 CFR 164.520(c)(1)(iii). For instance, if an employee of a firm and her three dependents are covered under a single health plan policy, that health plan can satisfy the reminder requirement by sending information concerning the availability of the Notice of Privacy Practices to just the employee, rather than to the employee and each dependent.

This information is especially timely as the third-anniversary of the compliance date of the HIPAA Privacy Rule nears. Health plans, other than small health plans, were first required to distribute their Notice of Privacy Practices to subscribers and enrollees by April 14, 2003. Thus, those health plans that have not already reminded subscribers and enrollees in some manner of the availability of their Notice of Privacy Practices and how they may obtain a copy, must do so no later than April 14, 2006. For small health plans, which had until April 14, 2004, to first distribute their Notices of Privacy Practices, the compliance date for the triennial reminder notice requirement is April 14, 2007. These plans can begin to prepare now to meet this requirement using the most efficient means, such as including the reminder notice of the availability of the Notice of Privacy Practices in open enrollment materials, a group health plan newsletter provided to all members, or similar all-member mailings.
May a health plan disclose protected health information to a person who calls the plan on the beneficiary’s behalf?

Answer

Yes, subject to the conditions set forth in 45 CFR 164.510(b) of the HIPAA Privacy Rule. The Privacy Rule at 45 CFR 164.510(b) permits a health plan (or other covered entity) to disclose to a family member, relative, or close personal friend of the individual, the protected health information (PHI) directly relevant to that person’s involvement with the individual’s care or payment for care. A covered entity also may make these disclosures to persons who are not family members, relatives, or close personal friends of the individual, provided the covered entity has reasonable assurance that the person has been identified by the individual as being involved in his or her care or payment.

A covered entity only may disclose the relevant PHI to these persons if the individual does not object or the covered entity can reasonably infer from the circumstances that the individual does not object to the disclosure; however, when the individual is not present or is incapacitated, the covered entity can make the disclosure if, in the exercise of professional judgment, it believes the disclosure is in the best interests of the individual.

For example:

- A health plan may disclose relevant PHI to a beneficiary’s daughter who has called to assist her hospitalized, elderly mother in resolving a claims or other payment issue.

- A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm for the plan that the representative calling is assisting the beneficiary.

- A health plan may disclose relevant PHI to a Congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the Congressional office’s assistance.

- A Medicare Part D plan may disclose relevant PHI to a staff person with the Centers for Medicare and Medicaid Services (CMS) who contacts the plan to assist an individual regarding the Part D benefit, if the information offered by the CMS staff person about the individual and the individual’s concerns is sufficient to reasonably satisfy the plan that the individual has requested the CMS staff person’s assistance.

Last revised: March 26, 2007
Health Information Privacy

Is a software vendor a business associate of a covered entity?

Answer:

The mere selling or providing of software to a covered entity does not give rise to a business associate relationship if the vendor does not have access to the protected health information of the covered entity. If the vendor does need access to the protected health information of the covered entity in order to provide its service, the vendor would be a business associate of the covered entity.

For example, a software company that hosts the software containing patient information on its own server or accesses patient information when troubleshooting the software function, is a business associate of a covered entity. In these examples, a covered entity would be required to enter into a business associate agreement before allowing the software company access to protected health information. However, when an employee of a contractor, like a software or information technology vendor, has his or her primary duty station on-site at a covered entity, the covered entity may choose to treat the employee of the vendor as a member of the covered entity’s workforce, rather than as a business associate. See the definition of “workforce” at 45 CFR 160.103.
Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

Answer:

No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected health information to a conduit is very small, a conduit is not a business associate of the covered entity.