Brought to you by Ardent Solutions

HIPAA Privacy Common Questions

When did the HIPAA Privacy Rule become effective?

Most covered entities had until April 14, 2003, to comply. Small health plans—those with annual receipts of $5 million or less—had an additional year to comply, until April 14, 2004.

What does the HIPAA Privacy Rule accomplish?

The HIPAA Privacy Rule restricts how patients' personally identifiable health information may be used and disclosed by certain organizations. While some states have laws that protect patients' privacy, this federal regulation establishes a minimum level of privacy protections that must be given to all patients' medical records. In summary, the regulation:

- Requires that patients be told how their medical records will be used and disclosed;
- Sets limits on how patients' medical records may be used and disclosed; and
- Imposes fines where the requirements contained within the regulations are not followed.

Who is governed by the HIPAA Privacy Rule?

The following organizations are governed by this regulation:

- Health plans;
- Health care clearinghouses; and
- Health care providers that conduct certain transactions electronically.

The HIPAA Privacy Rule makes clear that neither the employer nor a plan sponsor is directly regulated. Instead, the health plan is regulated. Where the plan sponsor has access to protected health information (PHI) related to the administration of the health plan, it must comply with the administrative requirements of the HIPAA Privacy Rule. A plan sponsor's access to enrollment applications and disenrollment information ALONE does not qualify as having access to PHI for purposes of the rules.

Some of the HIPAA Privacy Rule applies directly to business associates. The rule also includes a list of provisions which must be contained within a business associate contract. The mandatory provisions require the business associate to comply with many, but not all, of HIPAA's requirements.

Who is not governed by the HIPAA Privacy Rule?

Self-administered, self-funded group health plans with fewer than 50 participants are not required to comply with the HIPAA Privacy Rule.

The following benefits are not subject to the HIPAA Privacy Rule:

- Accident only;
- Disability income;

- Liability insurance;
- Life insurance; and
- Workers' compensation.

Note: The benefits excluded under the Privacy Rule differ from those excluded under HIPAA's portability and nondiscrimination rules (for example, limited scope dental and vision plans ARE subject to the HIPAA Privacy Rule).

Can an entity opt out of the HIPAA Privacy Rule?

No. While HIPAA allowed non-federal, self-funded non-governmental plans to opt out of HIPAA's requirements related to nondiscrimination, special enrollment and pre-existing conditions prior to health care reform, covered entities were never permitted to opt out of the HIPAA Privacy Rule.

What information is governed by the HIPAA Privacy Rule?

The rules govern all forms of PHI (oral, paper and electronic) when it is used or disclosed by a covered entity.

Under the HIPAA Privacy Rule, can individuals sue if their privacy rights are violated?

The HIPAA Privacy Rule does not provide a private right to sue. The Department of Health and Human Services' (HHS) Office of Civil Rights has the authority to accept and investigate complaints and conduct compliance reviews. The HIPAA Privacy Rule includes both civil and criminal sanctions for failure to comply.

While the HIPAA Privacy Rule does not directly provide a private right to sue, an individual may have other legal remedies, including:

- ERISA remedies where a plan has failed to follow provisions within its plan documents;
- Breach of contract remedies;
- Violation of state privacy laws; and
- Professional sanctions (for example, accountants, attorneys and physicians).

Under the HIPAA Privacy Rule, what provisions must be included within a business associate contract?

The HIPAA Privacy Rule requires that a covered entity receive satisfactory assurances from the business associate that it will appropriately handle PHI. The regulations specify the elements of satisfactory assurances that must be contained within a business associate contract.

A business associate contract must establish the permitted and required uses and disclosures of PHI by the business associate.* It must also require the business associate to:

- Implement appropriate safeguards (for example, limit access to employees with a need to know);
- Report to the covered entity any known use or disclosure of PHI not permitted by the contract or any breach of unsecured PHI;
- Ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the business associate agree to the same restrictions that apply to the business associate;
- Make PHI available, including for amendment, to individuals as required by the rules;
- Maintain an accounting of disclosures, made during the last six years, and make the accounting available upon request; and

10/10, EM 6/15

- Make its internal practices, books and records relating to use and disclosure of PHI available to HHS.

The business associate contract must also allow the covered entity to terminate the contract in the event of a material breach. At termination, the business associate must be required to destroy or return all PHI, if feasible, or extend the limitations on use and disclosure beyond termination of the contract.

Also, a business associate that uses a subcontractor is required to enter into a business associate contract with the subcontractor.

*The business associate may not be permitted to use or further disclose PHI in a manner that would violate HIPAA if done by the covered entity.

Note: Although a business associate contract is often required by HIPAA where a third party has access to PHI, provisions that are not required to be included should be reviewed carefully and are negotiable (for example, indemnification).

Under the HIPAA Privacy Rule, what information must be included in all authorizations?

The following information must be contained—in plain language—within all authorizations:

1. A description of the information to be used or disclosed, with sufficient specificity to allow the covered entity to know what information the authorization references;
2. The name or other specific identification of the person/class of persons that are authorized to release the PHI;
3. The name or other specific identification of the person/class of persons that are authorized to receive the PHI;
4. A description of the purpose of the requested use or disclosure (for example, at the request of the individual);
5. An expiration date or event;
6. A statement that the individual has a right to revoke an authorization in writing and an explanation of the procedures for revocation together with:
    - The exceptions to the right to revoke; or
    - A reference to the privacy notice if it contains an explanation of the individual's right to revoke;
7. An explanation of the covered entity's ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the receipt of an authorization;
8. A statement that informs the individual that the information used or disclosed pursuant to the authorization is subject to re-disclosure by the recipient and may no longer be protected by the HIPAA Privacy Rule; and
9. The individual's signature and date of signature.

If the authorization is signed by a personal representative of the individual, the representative must indicate his or her authority to act for the individual. The individual should be provided with a copy of the signed authorization.

An authorization for research purposes is not required to include an expiration date, but the form must indicate that the authorization does not expire. An authorization to sell PHI must state that the disclosure will result in remuneration to the covered entity. Also, if a marketing disclosure involves financial remuneration, the authorization must state that remuneration is involved.

10/10, EM 6/15

HIPAA Privacy Common Questions

Under the HIPAA Privacy Rule, can an authorization be combined with another document signed by an individual?

An authorization may not be combined with another document signed by an individual, but it can generally be combined with another authorization. However, where an authorization is related to use and disclosure of PHI for research purposes, the authorization may be combined with an individual's consent to participate in the research study.

Under the HIPAA Privacy Rule, what provisions must be included within a data use agreement?

The HIPAA Privacy Rule requires that a covered entity receive satisfactory assurances from the recipient of a limited data set that it will appropriately handle the information provided. The regulations specify the satisfactory assurances that must be contained within a data use agreement. They are:

1. Establish permitted and required uses and disclosures of the limited data set by the recipient;*
2. Establish who is permitted to use and receive the limited data set;
3. Provide that the limited data set recipient will:
    - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
    - Report to the covered entity any known use or disclosure of the information not provided for by its data use agreement;
    - Ensure that any agents, including a subcontractor, to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to the information; and
    - Not identify the information or contact the individuals.

*The limited data set recipient may not be permitted to use or further disclose the limited data set in a manner that would violate HIPAA if done by the covered entity.

Under the HIPAA Privacy Rule, may a health care provider disclose PHI about an individual to another provider when the information is requested for the treatment of a family member of the individual?

Yes. The HIPAA Privacy Rule permits a covered health care provider to use or disclose PHI for treatment purposes. While in most cases the treatment will be provided to the individual, the HIPAA Privacy Rule does allow the information to be used or disclosed for the treatment of others. Thus, the rule does permit a doctor to disclose PHI about a patient to another health care provider for the purpose of treating another patient. These uses and disclosures are permitted without the individual's written authorization or other agreement, with the exception of disclosures of psychotherapy notes, which requires the written authorization of the individual. However, the HIPAA Privacy Rule permits, but does not require, a covered health care provider to disclose the requested PHI. Thus, the doctor with the PHI may decline to share the information, even if the Rule would allow it.

The HIPAA Privacy Rule may also impose other limitations on these disclosures. Individuals have the right to request additional restrictions on the use or disclosure of PHI. If the health care provider has agreed to the requested restriction, then the doctor is bound by that agreement and would not be permitted to share the information (except in emergency treatment situations). However, the health care provider does not have to agree to the requested restriction.

10/10, EM 6/15

HIPAA Privacy Common Questions

Under the HIPAA Privacy Rule, when may a covered entity use and disclose PHI?

The HIPAA Privacy Rule allows covered entities to use and disclose PHI for treatment, payment or health care operations in the following ways:

1. For its own treatment, payment or health care operations;
2. For treatment activities of any health care provider;
3. For payment activities of another covered entity or any health care provider; and
4. For health care operations activities of another covered entity that has or had a relationship with the patient whose information is being disclosed.

Where use and disclosure of PHI is related to health care operations activities of another covered entity, health care operations activities are limited to:

- Quality assessment and improvement activities;
- Population-based activities relating to improving health or reducing health care costs;
- Case management and care coordination;
- Conducting training programs;
- Accreditation, licensing and credentialing activities; and
- Health care fraud and abuse detection or compliance.

In limited circumstances, the rules also allow covered entities to use and disclose PHI for purposes other than treatment, payment or health care operations, such as:

- Disclosures for workers' compensation;
- Prevention of serious threat to health or safety;
- Judicial or and administrative proceedings; and
- Public health activities.

The final modifications, released in August 2002, expanded the scope of permissible uses and disclosures of PHI by the covered entity. The HIPAA Privacy Rule requires an individual's authorization for uses and disclosures of PHI for purposes that are not otherwise permitted or required by law.

How does the HIPAA Privacy Rule impact our state law governing medical privacy?

The HIPAA Privacy Rule establishes a federal floor for privacy protections afforded to medical records. States may pass laws which provide greater protections to medical records. However, the HIPAA Privacy Rule preempt any state law that is contrary to these federal regulations. In short, where federal and state law both govern medical privacy, the law that provides the individual with greater protection applies.

While the scope of the HIPAA Privacy Rule is quite large, it is also possible that some state laws may apply to entities that would not otherwise be required to comply with HIPAA's requirements. Generally, self-funded health plans are exempt from state insurance laws that relate to employee benefit plans under current ERISA preemption analysis.

Employers should continue to be cognizant of other laws that govern privacy of medical information outside of the employee benefit plan arena, such as the Americans with Disabilities Act (ADA).

10/10, EM 6/15

HIPAA Privacy Common Questions

How does the HIPAA Privacy Rule impact an insurance carrier's ability to obtain medical histories during the underwriting process?

HIPAA allows an insurance carrier to continue to ask applicants questions regarding their medical history in order for it to assess its risk and establish the premium to be charged to the policyholder. However, HIPAA requires that a health care provider be provided with an authorization signed by the applicant before the health care provider can provide the insurance carrier with any medical information related to the applicant. HIPAA requires that the insurance carrier request only the minimum necessary amount of information. If insurance is not placed with the insurance carrier, HIPAA prohibits the carrier from further using the PHI, except as permitted by law.

Also, effective Sept. 23, 2013, HIPAA prohibits health plans from using or disclosing PHI that is genetic information for underwriting purposes (long-term care plans are exempt), as required by the Genetic Information Nondiscrimination Act of 2008 (GINA).

What are an individual's rights under the HIPAA Privacy Rule?

The rights provided to an individual under HIPAA include:

- A right to inspect or obtain a copy of his or her PHI;
- A right to amend or correct inaccuracies in his or her PHI;
- A right to obtain an accounting of disclosures made of his or her PHI;
- A right to receive a privacy notice;
- A right to request restrictions on the use and disclosure of his or her PHI;
- A right to request confidential communications of his or her PHI; and*
- A right to challenge use of his or her own PHI through the complaint processes established by a) the covered entity and b) the Secretary of HHS.

*Covered health care providers are required to accommodate reasonable requests by patients about how PHI is communicated to the patient. For example, an individual who does not want his or her family to know about a certain treatment may request that the provider communicate with the individual at his or her place of employment or send communications to an alternate address.

In addition, effective Sept. 23, 2013, covered entities must:

- Provide an individual with access to PHI in the electronic form and format requested by the individual if the PHI is maintained electronically in one or more designated record sets; and
- Agree to an individual's request to restrict PHI if the information pertains to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid in full.

Does the HIPAA Privacy Rule limit an individual's ability to gather and share family medical history information?

No. The HIPAA Privacy Rule may limit how a covered entity (for example, a health plan or most health care providers) uses or discloses individually identifiable health information, but does not prevent individuals themselves from:

- Gathering medical information about their family members; or
- Deciding to share this information with family members or others, including their health care providers.

10/10, EM 6/15

Thus, individuals are free to provide their doctors with a complete family medical history or communicate with their doctors about conditions that run in the family.

Does the HIPAA Privacy Rule limit what a doctor can do with a family medical history?

Yes, if the doctor is a "covered entity" under the HIPAA Privacy Rule. A doctor who conducts certain financial and administrative transactions electronically is considered a covered health care provider. The HIPAA Privacy Rule allows a covered health care provider to use or disclose PHI (other than psychotherapy notes), including family history information, for treatment, payment and health care operation purposes without obtaining the individual's written authorization or other agreement.

The HIPAA Privacy Rule also generally allows covered entities to disclose PHI without obtaining the individual's written authorization or other agreement for certain purposes to benefit the public (for example, circumstances that involve public health research or health oversight activities). When a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual's family medical history, this information becomes part of the individual's medical record and is treated as PHI. Thus, the individual (and not the family members included in the medical history) may exercise the rights under the HIPAA Privacy Rule to this information in the same fashion as any other information in the medical record.

What do the HIPAA Privacy and Security rules require of covered entities when they dispose of PHI?

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical and physical safeguards to protect the privacy of PHI, in any form. This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of the information.

In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI. Covered entities must also ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member. Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers.

Thus, covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. However, the privacy and security rules do not require a particular disposal method. Covered entities must review their own circumstances to determine what steps are reasonable to safeguard PHI through disposal, and develop and implement policies and procedures to carry out those steps.

In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the form, type and amount of PHI to be disposed. For instance, the disposal of certain types of PHI (such as name, social security number, driver's license number, debit or credit card number, diagnosis, treatment information or other sensitive information) may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual's reputation.

In general, examples of proper disposal methods may include, but are not limited to:

- For PHI in paper records, shredding, burning, pulping or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable and otherwise cannot be reconstructed.
- Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.

10/10, EM 6/15

- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) or destroying the media (disintegration, pulverization, melting, incinerating or shredding).

For more information on proper disposal of electronic PHI, see the HHS website.

Other methods of disposal also may be appropriate, depending on the circumstances. Covered entities are encouraged to consider the steps that other prudent health care and health information professionals are taking to protect patient privacy in connection with record disposal. In addition, if a covered entity is winding up a business, the covered entity may wish to consider giving patients the opportunity to pick up their records prior to any disposition by the covered entity (and note that many states may impose requirements on covered entities to retain and make available for a limited time, as appropriate, medical records after dissolution of a business).

May a covered entity dispose of PHI in dumpsters accessible by the public?

No, unless the PHI has been rendered essentially unreadable, indecipherable and otherwise cannot be reconstructed prior to it being placed in a dumpster. In general, a covered entity may not dispose of PHI in paper records, labeled prescription bottles, hospital identification bracelets, PHI on electronic media or other forms of PHI in dumpsters, recycling bins, garbage cans or other trash receptacles generally accessible by the public or other unauthorized persons.

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical and physical safeguards to protect the privacy of PHI, in any form, including in connection with the disposal of the information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. Depositing PHI in a trash receptacle generally accessible by the public or other unauthorized persons is not an appropriate privacy or security safeguard. Instead, covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI. Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

For example, depending on the circumstances, proper disposal methods may include (but are not limited to):

- Shredding or otherwise destroying PHI in paper records so that the PHI is rendered essentially unreadable, indecipherable and otherwise cannot be reconstructed prior to it being placed in a dumpster or other trash receptacle.
- Maintaining PHI for disposal in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- In justifiable cases, based on the size and the type of the covered entity and the nature of the PHI, depositing PHI in locked dumpsters that are accessible only by authorized persons, such as appropriate refuse workers.
- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) or destroying the media (disintegration, pulverization, melting, incinerating or shredding).

May a covered entity hire a business associate to dispose of PHI?

Yes, a covered entity may, but is not required to, hire a business associate to appropriately dispose of PHI on its behalf. In doing so, the covered entity must enter into a contract or other agreement with the business associate that requires the business associate, among other things, to appropriately safeguard the PHI through disposal. Thus, for example, a covered entity may hire an outside vendor to pick up PHI in paper records or on electronic media from its

10/10, EM 6/15

premises, shred, burn, pulp or pulverize the PHI, or purge or destroy the electronic media, and deposit the deconstructed material in a landfill or other appropriate area.

How should home health workers or other workforce members of a covered entity dispose of PHI that they use off of the covered entity's premises?

The HIPAA Privacy Rule requires that covered entities develop and apply policies and procedures for appropriate administrative, technical and physical safeguards to protect the privacy of PHI, including through final disposition. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored. The rules are flexible and thus do not specify particular types of disposal methods; however, covered entities must ensure that the disposal method reasonably protects against impermissible uses and disclosures of PHI and protects against reasonably anticipated threats or hazards to the security of electronic PHI.

Whatever the disposal method, a covered entity must ensure that appropriate workforce members, either working on the premises or off-site, receive training on and follow the disposal policies and procedures of the covered entity. These policies and procedures could require, for example, that employees or other workforce members who use PHI off-site, including electronic PHI, return all PHI to the covered entity for appropriate disposal. Or, for example, if appropriate under the circumstances, a covered entity could give off-site workforce members the option of either properly shredding PHI in paper records themselves or returning the PHI to the covered entity for disposal. In cases where workforce members fail to comply with the covered entity's disposal policies and procedures, the covered entity must apply appropriate sanctions.

May a covered entity reuse or dispose of computers or other electronic media that store electronic PHI?

Yes, but only if certain steps have been taken to remove the electronic PHI (ePHI) stored on the computers or other media before its disposal or reuse, or if the media itself is destroyed before its disposal. The HIPAA security rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of ePHI from electronic media before the media are made available for reuse. Depending on the circumstances, appropriate methods for removing ePHI from electronic media prior to reuse or disposal may be by clearing (using software or hardware products to overwrite media with non-sensitive data) or purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains) the information from the electronic media. If circumstances warrant the destruction of the electronic media prior to disposal, destruction methods may include disintegrating, pulverizing, melting, incinerating or shredding the media. Covered entities may contract with business associates to perform these services for them.

Does the HIPAA Privacy Rule require covered entities to keep patients' medical records for any period of time?

No, the HIPAA Privacy Rule does not include medical record retention requirements. Rather, state laws generally govern how long medical records are to be retained. However, the HIPAA Privacy Rule does require that covered entities apply appropriate administrative, technical and physical safeguards to protect the privacy of medical records and other PHI for whatever period the information is maintained by a covered entity, including through disposal.

10/10, EM 6/15