# Supplemental Information

## Patient Identifiers

- Patient Names
- Telephone Numbers
- Fax Numbers
- Social Security Numbers
- Vehicle Identifiers
- E-mail addresses
- Web URLS and IP addresses
- Dates
- Geographic Subdivisions
- Names of Relatives
- Full Face Photographs or Images
- Healthcare Record Numbers
- Account Numbers
- Biometric Identifiers (fingerprints or voiceprints)
- Device Identifiers
- Health Plan Beneficiary Numbers
- Certificate/license Numbers
- Any Other Unique Number, Code, or characteristic that can be linked to an individual

# Breach Notification Requirements

Breach notices to individuals must be made within 60 days and include:

- Description of what happened and dates
- Description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- Description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, e-mail address, website, or postal address
- Written notice to last known address
- If the individual is deceased, notification may be sent to the next of kin or personal representative of the individual
- Notification may be provided in one or more mailings as information becomes available
- In urgent situations, substitute notice may be provided by telephone, email or other means

If the covered entity does not have sufficient contact information for ten or more affected individuals, the following applies:

  - Conspicuous posting for 90 days on home page of covered entity's website or posting in print or broadcast media where the affected individuals may reside
  - Include a toll-free number that remains active for at least 90 days where individuals can learn if they were affected by the breach

If over 500 patient records are involved, you must:

- Immediately notify HHS
- Publish press release for local media
- Not doing so may be considered a criminal offense

**This has the potential to destroy your business!**

- If a breach involves 500 or more individuals, the covered entity must report the breach to HHS at the same time it notifies affected individuals
- If a breach involves less than 500 individuals, the covered entity will make an annual reporting of all such breaches discovered in a calendar year to HHS
- This data is collected for reporting to Congress

**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, such as electronically billing Medicare or other payers for health care services, is considered a covered health care provider. The HIPAA Privacy Rule limits how a covered health care provider may use or disclose protected health information. The HIPAA Privacy Rule allows a covered health care provider to use or disclose protected health information (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 protected health information 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 "protected health information" about the individual. 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, including the right of access, amendment, and the ability to authorize disclosure to others.

**If the patient is not present or is incapacitated, may a health care provider still share the patient's health information with family, friends, or others involved in the patient's care or payment for care?**

Yes. If the patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient. When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care. The health care provider may discuss only the information that the person involved needs to know about the patient's care or payment.

Here are some examples:

- A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.
- A pharmacist may give a prescription to a patient's friend who the patient has sent to pick up the prescription.
- A hospital may discuss a patient's bill with her adult son who calls the hospital with questions about charges to his mother's account.

- A health care provider may give information regarding a patient's drug dosage to the patient's health aide who calls the provider with questions about the particular prescription.

BUT:

- A nurse may not tell a patient's friend about a past medical problem that is unrelated to the patient's current condition.
- A health care provider is not required by HIPAA to share a patient's information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

**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?**

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 health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care 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.

**Does HIPAA require that a health care provider document a patient's decision to allow the provider to share his or her health information with a family member, friend, or other person involved in the patient's care or payment for care?**

No. HIPAA does not require that a health care provider document the patient's agreement or lack of objection. However, a health care provider is free to obtain or document the patient's agreement, or lack of objection, in writing, if he or she prefers. For example, a provider may choose to document a patient's agreement to share information with a family member with a note in the patient's medical file.

**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 Web site.

**Can the personal representative of an adult or emancipated minor obtain access to the individual's medical record?**

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.

**If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?**

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.

**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. 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.