October 2, 2002

Frequently Asked Questions
About the HIPAA Privacy Rule

Look for updates to these FAQs
-- as OCR responds to questions & comments received at its website --
and updated guidance on significant Privacy Rule topics, in the near future.

ONLINE AT: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html

- **If I believe that my privacy rights have been violated, when can I submit a complaint?**

  Response: 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 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 C.F.R. §§ 160.306 and 164.534. OCR will provide further information on its website 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?**

  Response: 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 C.F.R. § 164.524.

- **Does the Privacy Rule protect genetic information?**

  Response: 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.

- **Does the Rule create a government database with all individuals' personal health information?**

  Response: 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.

- **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 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?**

  Response: 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.

- **Can a physician's office FAX patient medical information to another physician's office?**

  Response: The 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 C.F.R. § 164.530(c).

- **Can physician offices use patient sign-in sheets or call out the names of patients in their waiting rooms?**

Response: Yes, covered entities such as physician 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 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. However, these "incidental" disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards (45 C.F.R. § 164.530(c)), and implemented the minimum necessary standard, where appropriate (45 C.F.R. §§ 164.502(b) and 164.514(d)). 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 more information, see the preamble to the final modifications to the Privacy Rule (67 Fed. Reg. 53182, 53193–95 (August 14, 2002)).

- **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 Privacy Rule allow the clinic to continue this practice?**

  Response: Yes, the HIPAA 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. 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 C.F.R. §164.530(c).

- **A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the Privacy Rule allow the hospital to continue this practice?**

  Response: 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 (45 C.F.R.§164.530(c)), and implemented the minimum necessary standard (45 C.F.R. §§164.502(b) and 164.514(d)). 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. For more information, see the preamble to the final modifications to the Privacy Rule (67 Fed. Reg. 53182, 53193– 95 (August 14, 2002)).

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

  Response: Yes, the 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 C.F.R. § 164.510(a).

- **How does the 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?**

  Response: 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 C.F.R. § 164.501 (definitions) and § 164.502(a)(1)(ii) (permitted disclosures).

- **Does the Privacy Rule permit covered entities or their collection agencies to obtain payment from parties other than the patient, e.g., from spouses or guardians?**

  Response: Yes, the Privacy Rule permits a covered entity, or a business associate acting on behalf of, or providing a service to, 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 C.F.R. § 164.506(c). 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 use or disclosure of PHI. See 45 C.F.R. § 164.502(b).

- **Is a physician or other provider going to be considered a business associate of a health plan or other payer?**

  Response: 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. A business associate relationship could arise if the provider is performing a function on behalf of, or providing services to, the health plan (e.g., case management services). See the discussions at 67 Fed. Reg. 14776, 14788 (March 27, 2002) concerning this issue.

- **Do hospitals or other covered entities need to monitor their business associates?**

  Response: No, the 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. However, if a covered entity finds out about a material violation of the contract, it must act to end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible, the covered entity must report the problem to the Office for Civil Rights. See 45 C.F.R § 164.504(e)(1).

- **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?**

  Response: 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 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 45 C.F.R § 160.501.

- **Are janitorial services business associates?**

  Response: Generally, janitorial services that clean the facilities of a covered entity (i.e., a health care provider, health plan or health care clearinghouse) 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 Privacy Rule. See 45 C.F.R. § 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. See 65 Fed. Reg. 82462, 82480 (December 28, 2000).

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

  Response: 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. See 65 Fed. Reg. 82462, 82476 (December 28, 2000).

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

  Response: 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. 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 C.F.R.§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 C.F.R. § 164.504 (a) – (c) for more information about hybrid entities.

- **Are the following types of insurance covered under HIPAA: long/short term disability; workers compensation; automobile liability that includes coverage for medical payments?**

  Response: 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 C.F.R. § 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.

- **Is an entity that is acting as a third party administrator to a group health plan a covered entity?**

  Response: 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 C.F.R. § 160.103.

- **The Social Security Administration (SSA) collects medical records for the Social Security Income (SSI) disability program. Is SSA a covered entity (e.g., a health plan)?**

  Response: 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. These terms are defined in detail at 45 C.F.R. § 160.103.

- **Is the Privacy Rule compliance date delayed by the Administrative Simplification Compliance Act (ASCA) that was enacted in December 2001?**

  Response: 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/.

- **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?"**

  Response: 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 C.F.R. § 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 C.F.R. § 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