MISCELLANEOUS
FREQUENTLY ASKED QUESTIONS
ABOUT THE HIPAA PRIVACY RULE

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

A: 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.

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

A: 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.

Q: Does the HIPAA Privacy Rule protect genetic information?

A: 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.

Q: 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?

A: 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.

Q: Can a physician's office FAX patient medical information to another physician's office?

A: 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 CFR164.530(c).

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

A: 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).

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

A: 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 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 164.504 (a) – (c) for more information about hybrid entities.

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

A: 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.

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

A: 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.

Q: 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)?

A: 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 CFR 160.103.

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

A: 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/.

Q: 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?"

A: 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.

Q: Does the HIPAA Privacy Rule require that covered entities provide patients with access to oral information?

A: 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.

Q: Does the HIPAA Privacy Rule require that covered entities document all oral communications?

A: 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.