Complying with the HIPAA Privacy Rule

The following is an overview that provides answers to general questions regarding the regulation entitled, Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), promulgated by the Department of Health and Human Services (HHS), and process for modifications to that rule. Detailed guidance on specific requirements in the regulation is presented at http://www.hhs.gov/ocr/hipaa, the Web site from which this page was taken.

The Privacy Rule provides the first comprehensive federal protection for the privacy of health information. All segments of the health care industry have expressed their support for the objective of enhanced patient privacy in the health care system. At the same time, HHS and most parties agree that privacy protections must not interfere with a patient's access to or the quality of health care delivery.

The guidance provided in this section is meant to communicate as clearly as possible the privacy policies contained in the rule. In some cases, the guidance identifies areas of the Privacy Rule where a modification or change to the rule is necessary. These areas are summarized below in response to the question "What changes might you make to the final rule?" and discussed in more detail at http://www.hhs.gov/ocr/hippa.

Frequently Asked Questions

Q: What does this regulation do?

A: The Privacy Rule became effective on April 14, 2001. Most health plans and health care providers that are covered by the new rule must comply with the new requirements by April 2003.

For the first time, the Privacy Rule 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 requires 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 what disclosures of their information have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It gives patients the right to examine and obtain a copy of their own health records and request corrections.

Q: Why is this regulation needed?

A: In enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress mandated the establishment of 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 current patchwork of laws, personal health information can be distributed--without either notice or consent--for reasons that have nothing to do with a patient's medical treatment or health care reimbursement. Patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card, or to an employer who may 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. But 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 all parties regarding protection of personal health information.

Q: What does this regulation require the average provider or health plan to do?

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

- Providing information to patients about their privacy rights and how their information can be used.
- Adopting clear 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 final 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 rules 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.

Q. Who must comply with these new privacy standards?

A: As required by Congress in HIPAA, the Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards are required to be adopted by the Secretary under HIPAA, such as electronic billing and fund transfers. These entities (collectively called "covered entities") are bound by the new privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. The law does not give 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. The "business associate" section of this guidance provides a more detailed discussion of the covered entities' responsibilities when they engage others to perform essential functions or services for them.

Q: When will covered entities have to meet these standards?

A: As Congress required in HIPAA, most covered entities have two full years from the date that the regulation took effect--or, until April 14, 2003--to come into compliance with these standards. Under the law, small health plans will have three full years--or, until April 14, 2004--to come into compliance.

The HHS Office for Civil Rights (OCR) will provide assistance to help covered entities prepare to comply with the rule. OCR maintains a Web site with information on the new regulation, including guidance for industry, such as these frequently asked questions, at http://www.hhs.gov/ocr/hipaa/.

Q: Do you expect to make any changes to this rule before the compliance date?

A: We can and will issue proposed modifications to correct any unintended negative effects of the Privacy Rule on health care quality or on access to such care.

In February 2001, Secretary Thompson requested public comments on the final rule to help HHS assess the rule's real-world impact in health care delivery. During the 30-day comment period, we received more than 11,000 letters or comments, including some petitions with thousands of names. These comments are helping to guide the Department's efforts to

clarify areas of the rule to eliminate uncertainties and to help covered entities begin their implementation efforts.

Q: What changes might you make in the final rule?

A: We continue to review the input received during the recent public comment period to determine what changes are appropriate to ensure that the rule protects patient privacy as intended without harming consumers' access to care or the quality of that care.

Examples of standards in the Privacy Rule for which we will propose changes are:

- Phoned-in Prescriptions--A change will permit pharmacists to fill prescriptions phoned in by a patient's doctor before obtaining the patient's written consent.
- Referral Appointments--A change will permit direct treatment providers receiving a first time patient referral to schedule appointments, surgery, or other procedures before obtaining the patient's signed consent.
- Allowable Communications--A change will increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high quality health care, including routine oral communications with family members, treatment discussions with staff involved in coordination of patient care, and using patient names to locate them in waiting areas.
- Minimum Necessary Scope--A change will increase covered entities' confidence that certain common practices, such as use of sign-up sheets and X-ray light boards, and maintenance of patient medical charts at bedside, are not prohibited under the rule.

In addition, HHS may reevaluate the Privacy Rule to ensure that parents have appropriate access to information about the health and well being of their children. This issue is discussed further in the "Parents and Minors" section of this guidance.

Other changes to the Privacy Rule also may be considered as appropriate.

Q: How will you make any changes?

A: Any changes to the final rule must be made in accordance with the Administrative Procedures Act (APA). HHS intends to comply with the APA by publishing its rule changes 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 final rule to implement appropriate modifications.

Congress specifically authorized HHS to make appropriate modifications in the first year after the final rule took effect in order to ensure the rule could be properly implemented in the real world. We are working as quickly as we can to identify where modifications are needed and what corrections need to be made so as to give covered entities as much time as possible to implement the rule. Covered entities can and should begin the process of implementing the privacy standards in order to meet their compliance dates.