On December 3, 2002, the US Department of Health and Human Services ("HHS"), Office of Civil Rights ("OCR"), released its most recent guidance (the "Guidance") addressing the HHS Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164 ("Privacy Rule") promulgated by HHS pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), title II, subtitle F, §§ 261-264, Public Law 104-191. This Guidance is but one installment in a cumulative series of guidance intended to address operational and implementation questions within the health care community and to encourage voluntary compliance with the Privacy Rule requirements. Although this installment does not address the full scope of provisions within the Privacy Rule, it is more comprehensive and detailed than previous OCR releases. The December 3, 2002 release includes a general overview of the Privacy Rule and includes the following topics:

- Incidental Uses & Disclosures
- Minimum Necessary Standards
- Personal Representatives
- Business Associates
- Uses & Disclosures for Treatment, Payment & Health Care Operations
- Marketing
- Public Health
- Research
- Workers' Compensation Laws
- Notice of Privacy Practices
- Government Access
- Miscellaneous FAQs

This article summarizes the Guidance and discusses some of its significant highlights. One important caveat: it is essential to keep in mind that all of the commentary, FAQs, audio conferences by HHS/CMS, this Guidance and any other unofficial government interpretations of the actual HIPAA regulations are just that -- unofficial. In other words, they do not represent the final, authoritative or definitive explanation of the regulations and should not be unequivocally relied upon. If (or when) the Privacy Rule is interpreted by a court, that court will decide how much, if any, weight these regulatory musings deserve. A judge may or may not be persuaded to accept the guidance from on high; however, it is just as likely that he/she may use an entirely different interpretation. Therefore, accept the Guidance as another tool for discovering the true meaning of the Rule, but do not consider it as the gospel truth.

MINIMUM NECESSARY & INCIDENTAL USE & DISCLOSURE

The Guidance regarding the minimum necessary standard and accountability for incidental uses and disclosures of protected health information ("PHI") is consistent with previous guidance from HHS on such topics as well as the commentary that preceded both the proposed and final modifications to the HIPAA privacy rule (the "Privacy Rule" or "Rule"). The underlying goal of the minimum necessary rule is to insure that covered entities have reasonable safeguards, policies and procedures in place to protect patient privacy. The minimum necessary requirement is not a strict standard; it is intended to make covered entities evaluate their current practices and implement protections, as needed, to prevent unnecessary disclosures of PHI. There is no expectation that the safeguards or minimum necessary policies and procedures will protect PHI from any and all potential risk. Incidental uses and disclosures of PHI are permissible as long as they are the byproducts of a use or disclosure that is in compliance with the Privacy Rule.

However, an incidental use or disclosure that results from a failure to comply with the minimum necessary standard or to implement reasonable safeguards designed to protect against such incidental use or disclosure is a violation of the Privacy Rule.

According to the Guidance, covered entities are not required to institute structural or systemic changes, such as encrypting wireless emergency radio communications or telephone systems in order to be in compliance with the Privacy Rule. The Privacy Rule does not prohibit providers from engaging in confidential conversations with other providers or with patients even if there is a possibility that the conversation could be overheard. HHS offers several examples of common practices that will remain permissible under the Rule, despite the risk of incidental disclosure to others, so long as reasonable safeguards are implemented to prevent unauthorized disclosures. For example, doctors would not be in violation of the Rule if they discussed lab results with their patients in a joint treatment area so long as reasonable precautions, such as talking in lowered voices or standing a distance away from others, were taken to prevent unauthorized disclosure of PHI.

BUSINESS ASSOCIATES

Definition of a "Business Associate."

Commentators have expressed a wide array of opinions about precisely what functions or activities a person or entity must engage in to qualify as a business associate under the Privacy Rule. Some commentators have identified business associates as those entities that engage in "covered functions" for, or on behalf of, a covered entity. While others have defined business associates as persons or entities that perform any function or activity for, or on behalf of, a covered entity so long as the function or activity involves the use or disclosure of PHI.

The Guidance offers yet another slightly more definitive interpretation of the term "business associate." According to OCR, a business associate is a person or entity that performs certain specific functions, activities or services that involve the use or disclosure of PHI on behalf of a covered entity. The types of functions or activities that could make a person or entity a business associate include payment or health care operations activities, such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, repricing and any other function or activity regulated by the Administrative Simplification Rules. This is in contrast to "covered functions," which the Rule defines as those functions performed by health plans, health care providers, or health care clearinghouses that make them covered entities. Business associate services are those legal, actuarial, accounting, consulting, data aggregation, management, administrative accreditation and financial services that involve the use or disclosure of PHI on behalf of a covered entity.

Transition Period for Existing Contracts.

The modifications to the Privacy Rule made in August 2002, included changes to the business associate requirements. Business associate contracts in existence prior to October 15, 2002 are not required to be in compliance with the Privacy Rule until one year after the April 14, 2003 compliance date, or until such contracts are renewed or modified, whichever occurs first (such contracts are referred to as "Transition Period Contracts"). The change was designed to ease some of the administrative and financial burdens on covered entities associated with re-negotiating existing agreements. But instead of making it easier for covered entities to be in compliance with the Rule, the transition period adds a new layer of complexity and administrative headache for covered entities and business associates alike.

According to the Guidance, some, but not all, of the compliance obligations under the Privacy Rule are applicable to business associates that perform functions pursuant to the terms of Transition Period Contracts. The Guidance states that covered entities have the following obligations with respect to PHI held by any such business associate: (a) PHI must be made available to the Secretary of HHS as necessary for the Secretary to determine if the covered entity is in compliance with HIPAA; (b) PHI maintained by any such business associate in a designated records set must be made available to fulfill an individual's right to access and amend her PHI; and (c) covered entities must mitigate, to the extent practicable, any harmful effect of an impermissible use or disclosure of PHI by the business associate. In spite of these obligations, the Guidance goes on to say that there is absolutely no requirement for covered entities to obtain satisfactory assurance from the business associate that it will appropriately safeguard the PHI in its possession. It is not clear exactly how a covered entity will be able to fulfill these obligations under HIPAA in the absence of any legal obligation for business associates to cooperate and work with the covered entity.

Moreover, the transition period creates additional problems of keeping track of which business associate contracts are HIPAA compliant and which are under the transition rules. It is entirely conceivable that a single business associate may have entered into numerous contracts with the same covered entity over a period of time, some of which will now have to comply with all of the HIPAA requirements for business associate relationships, and some of which will not. The safest course of action, if time and resources permit, is to re-negotiate as many Transition Period Contracts as possible prior to the April 14, 2003 compliance date.

Software Vendors.

Merely selling or providing software to a covered entity is not sufficient to establish a business associate relationship. According to the Guidance, in order to qualify as a business associate, the software vendor must need access to the covered entities' PHI in order to provide its service. For example, a software vendor that hosts, on its own server, the software containing a covered entity's patient information, is a business associate of that covered entity. Under the Rule, if an independent contractor or employee of a software vendor has an assigned workstation on a covered entity's premises and performs a substantial proportion of their activities at that location, then the covered entity may choose to treat that employee or independent contractor as either a business associate or as part of the workforce. If there is no business associate contract, then HHS will assume that the independent contractor is a member of the covered entity's workforce.

However, one significant problem with granting workforce status to such third partes is that the covered entity then assumes additional liability for any acts or omissions of such employee or independent contractor, to the extent that they are in violation of HIPAA. Executing a business associate contract helps shift the risk of noncompliance away from the covered entity and back to the third party, who may be in a better position to protect against the risk of its own failure to comply with HIPAA, in accordance with the terms of the business associate agreement. Moreover, HHS has consistently stated that covered entities are not required to monitor or oversee the extent to which its business associates abide by the privacy requirements under business associate contracts. The same cannot be said for those individuals or entities deemed to be a part of a covered entity's workforce.

ORGANIZED HEALTH CARE ARRANGEMENT

Unlike an affiliated covered entity, which adopts such a designation for the purpose of complying with the Rule, the Guidance seems to suggest that an organized health care arrangement ("OHCA") is not a discretionary arrangement. Instead (and contrary to what has been the generally accepted view), OCR implies that the OHCA arrangement automatically exists, without any affirmative action on the part of its participants, anytime a group of covered entities is part of an interaction that falls within the definition of an organized health care arrangement under the Rule. For example, according to the Guidance, an OHCA inevitably arises:

- In health care facilities where physicians and other providers (e.g., hospital staff with privileges, physicians visiting their patients at a residential facility) who have offices elsewhere also provide services at the facility.

- With respect to individuals jointly served by a health insurance issuer or HMO and the group health plan to which it provides health insurance or health coverage.

This view represents a striking departure from the conventional wisdom expressed by many commentators who understood an OHCA to be an optional tool that covered entities could deliberately and affirmatively structure as part of their efforts to achieve compliance with the Privacy Rule.

USES & DISCLOSURES FOR TREATMENT, PAYMENT, & HEALTH CARE OPERATIONS

Debt Collection.

The Guidance states that covered entities either directly, or indirectly, through collection agencies, may disclose PHI as necessary to obtain payment for health care. There is no limit to whom such disclosures may be made. Accordingly, persons other than the individual may be contacted by covered entities in order to obtain payment for health care services. Why is this permissible under the Rule? Because it falls under the definition of "payment." The Privacy Rule permits covered entities to use and disclose PHI for the purposes of treatment, payment or in support of their healthcare operations. It is important to remember however, that the minimum necessary rule is applicable to any such communication. Therefore, the amount of PHI disclosed must be limited to that amount that is reasonably necessary to achieve the purpose of the disclosure.

MARKETING

Disease Management, Health Promotion, Preventive Care and Wellness Programs.

Generally these activities do not fall under the definition of marketing under the Rule. For example, a hospital could start a program to prevent the onset of type II diabetes in teenagers and send a flyer to all teenaged patients who had been seen in the hospital during the previous 12 months and who have one or more risk factors for the disease, even if those individuals were not specifically seen for treatment of such risk factors or symptoms when they were in the hospital. Disease management and wellness programs operated directly by the covered entity or by a business associate on the covered entity's behalf, similarly do not constitute marketing, because they are communications about the covered entity's own health-related services. Communications by a covered entity about its own health-related services are specifically excluded from the definition of "marketing" under the Rule.

Remuneration for Treatment-Related Communications.

The Privacy Rule purports to give individuals important control over the use and disclosure of their PHI for the purpose of marketing. Generally, the Rule requires covered entities to obtain prior written authorization before making any use or disclosure of an individual's PHI for marketing purposes. However, the Guidance highlights some important exceptions to the general marketing requirements under the Rule. For example, the Privacy Rule is not violated when a covered entity is paid in exchange for sending out prescription refill reminders without obtaining prior patient authorization and disclosing the fact that the communication was made in exchange for payment. Communications such as prescription refill reminders are deemed to constitute "treatment" under the Rule and are therefore, excluded from the definition of marketing. For that reason, if a covered entity receives remuneration in exchange for such communication, there is no disclosure requirement as there would be if the communication constituted marketing. It is permissible for a covered entity to receive payment in exchange for treatment-related communications under the Privacy Rule. Accordingly, health care providers may also accept payment from pharmaceutical companies in exchange for recommending alternate medications to patients.

PUBLIC HEALTH

The Privacy Rule permits covered entities to disclose PHI, without obtaining authorization, to public health authorities legally authorized to receive such reports for specified public health purposes, including the prevention and control of disease, injury or disability. See 45 C.F.R. § 164.512(b). Public Health Authorities include state and federal agencies responsible for public health matters. See 45 C.F.R. § 164.501. The FDA and OSHA are included within that scope.

In general, the minimum necessary standard applies to disclosures of PHI, such that covered entities are required to limit within reason the amount of information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. The minimum necessary standard does not apply to disclosures by covered entities made pursuant to an authorization, or if otherwise required by law, in situations involving reporting associated with child abuse or neglect, FDA product regulation and safety, disease control and workplace medical surveillance.

The December 3, 2002 Guidance offers a series of responses to questions related to disclosures of PHI to public health authorities. A significant topic addresses whether a health care provider is obligated to obtain permission from a patient prior to notifying a public health authority of the occurrence of a reportable disease. OCR's answer is "No," reasoning that: (i) all states have laws that require providers to report cases of specific diseases to public health authorities; and (ii) the Privacy Rule specifically permits disclosures required by law. In the interest of protecting the public, and specifically to prevent further spread of disease, public health officials are often required to obtain information about persons affected by a disease. The result in this case is that the rule reflects policy that favors disclosure of information when in the public interest.

Consistent with this theme, OCR also addresses whether covered entities are permitted to disclose for public health purposes facially-identifiable PHI, such as name, address, and Social Security number. OCR's response to this question is in the affirmative, reasoning that, even if the disclosure is not required by law, covered entities may disclose, without authorization, information that is reasonably limited to that which is minimally necessary to accomplish the intended public purpose of the disclosure. For routine or recurring disclosures, OCR advises that a covered entity may develop protocols as part of its minimum necessary policies and procedures to address the type and amount of information that may be disclosed for such purposes.

OCR takes the opposite position with respect to disclosures to private entities for private

purposes, addressing whether covered entities are permitted to disclose PHI without authorization to a product manufacturer regulated by the FDA for use by the manufacturer to assess the effectiveness of its marketing campaign. OCR's unambiguous position is that such disclosures are absolutely prohibited, reasoning that disclosures to the FDA are solely for public health purposes, which are intended to facilitate the flow of information that is essential to the FDA's public health mission. On the contrary, disclosure of PHI to a private company (albeit FDA-regulated) for its own commercial purposes, or for any other non-public health purpose, is not permitted without an authorization. However, the Privacy Rule permits covered entities to continue to disclose PHI as necessary under current voluntary reporting of adverse events and to make similar reports that are necessary to ensure the quality, safety or effectiveness of an FDA-regulated product.

RESEARCH

The Privacy Rule permits covered entities to use and disclose PHI for research purposes with individual authorization and without authorization under limited circumstances. In the Guidance, OCR responds to several inquiries related to uses and disclosures of PHI for research purposes. Among them, OCR considers whether the Privacy Rule prohibits researchers from conditioning participation in a clinical trial on authorization to use or disclose PHI. OCR's conclusion is that the Privacy Rule does not prohibit researchers from conditioning enrollment in a research study on receipt of an authorization for the use of pre-existing health information, since the Rule does not even address conditions for enrollment in research studies.

The Guidance attempts to clarify some of the rules governing the creation and use of databases for research purposes. OCR explains that the Rule permits such research databases for current research without individuals' authorizations, if an Institutional Review Board ("IRB") or Privacy Board has granted a waiver. Furthermore, a covered entity may use the research database for future research studies if individual authorizations are obtained or there is an additional IRB or Privacy Board waiver. Also, with respect to existing databases or repositories created prior to the April 14, 2003 compliance date, without either patient permission or a waiver of informed consent by an IRB, OCR tells us that covered entities may continue to use or disclose PHI from such databases only if they obtain individual authorization or appropriate waivers.

OCR also considers a research participant's right of access to research records and results. The Guidance states that, with few exceptions, the Privacy Rule offers patients the right to inspect and obtain a copy of health information about them that is maintained by a covered entity or its business associate in a "designated record set" (i.e., a group of records which a covered entity uses to make decisions about individuals, including medical and billing records, enrollment, payment, claims adjudication and case management records). OCR recognizes that it is unlikely that a researcher would maintain a designated record set, but to the extent that it does so, such information would be accessible to research participants unless an exception under the Privacy Rule applies, such as a temporary suspension of the right of access while the clinical trial is in progress.

The Guidance addresses whether the Privacy Rule is in harmony with the Clinical Improvements Amendments of 1988 ("CLIA"). OCR responds in the affirmative and states that the Privacy Rule does not require clinical laboratories that are also covered entities to offer an individual access to information if CLIA prohibits them from doing so. Because CLIA permits clinical laboratories to provide clinical laboratory test records and reports only to "authorized persons" pursuant to state law, the test subject is not included as an authorized person. The result is that the Privacy Rule includes an exception to the general right of an individual to access PHI if such access is in conflict with CLIA.

OCR provides a straightforward answer to the question of when is a researcher also a covered

health care provider: when the researcher furnishes health care services to individuals (including research subjects) and transmits health information in electronic form in connection with a HIPAA transaction. The Guidance offers an example of researchers who provide health care to individuals, but have a hospital or billing service conduct electronic transactions on their behalf. Such researchers are covered entities for HIPAA purposes.

Researchers and covered entities have anxiously awaited clarification of the rules on preparatory research and recruitment of individuals into a research study. As is often the case, the clarifying FAQs are likely to shed as much heat as light on this complicated subject, and will certainly form the basis of many interesting articles and discussions. Here is what the Guidance says: Covered entities may use or disclose PHI for purposes preparatory to research, such as to aid study recruitment, as long as the researcher does not remove such PHI from the covered entity's site. Also, if the researcher is an employee or a member of the covered entity's workforce, he/she could use PHI to identify and contact prospective research subjects. OCR also notes that since the Rule permits a covered entity to disclose PHI to the individual who is the subject of the information, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an IRB or Privacy Board waiver of the authorization.

However (this is the interesting part), a researcher who is not a part of the covered entity may not use the preparatory research provision to contact prospective research subjects. In this case, OCR advises that the outside researcher would have to obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board in order to recruit potential research subjects.

WORKERS' COMPENSATION LAWS

The Privacy Rule is not applicable to organizations that include either (i) workers' compensation insurers, workers' compensation administrative agencies, or (ii) employers, unless they are otherwise covered entities. Access to health information for work-related illness is typically governed by state law and, because there is a significant degree of variability among such laws, the Privacy Rule permits disclosures of health information for workers' compensation purposes. Like the rule as applied to uses and disclosures for research purposes, disclosures for work-related illness are permitted without individual authorization in certain limited contexts and with authorization in other situations.

In the Guidance, OCR considers whether the Privacy Rule establishes an individual right to restrict the type or amount of information disclosed for workers' compensation purposes. OCR notes that the Rule does not provide individuals with a right to request restrictions on disclosures of information for workers' compensation purposes when that disclosure is required by law or authorized by, and necessary to comply with, a workers' compensation or similar law.

OCR also addresses several issues associated with compliance with workers' compensation state law requirements. The OCR Guidance states that the Privacy Rule always permits a covered entity to disclose PHI as necessary to comply with state law and, in these cases, no minimum necessary determination is required.

NOTICE OF PRIVACY PRACTICES

The Privacy Rule has established a panoply of individual rights associated with the use and disclosure of sensitive health information. The mechanism that will be used to inform patients of these rights takes the form of a notice called the Notice of Privacy Practices, to be developed and implemented by covered entities on an individual entity basis.

The Guidance responds to a series of operational questions associated with provider use of the notice. Specifically, OCR considers whether hospitals and other health care providers are required to provide notice to patients being treated in an emergency. OCR responds that hospitals and providers with a direct treatment relationship with the individual are not required to provide notices to patients at the time they are providing emergency treatment. The Rule requires providers to provide such notice only when it is practical to do so after the emergency has ended. In these circumstances, providers are not required to make a good-faith effort to obtain the patient's written acknowledgment of receipt of the notice.

The Guidance also addresses whether covered entities are permitted to distribute their notices as part of regular mailings. OCR responds in the affirmative, stating that no special or separate mailing is required to satisfy the Rule's distribution requirements. In fact, if the covered entity makes regular informative distributions via email, the email distribution of the notice will be sufficient, even if the email contains additional information.

OCR also deals with the issue of whether health care providers are required to obtain a new acknowledgment of receipt of the notice from patients if the entity changes its privacy policy. OCR's welcome answer is "No," since a covered health care provider with a direct treatment relationship with an individual is only required to make a good faith effort to obtain an individual's acknowledgment of receipt of the notice on the first occasion that the provider gives the notice to the individual, which is typically a the first instance that services are rendered.

GOVERNMENT ACCESS

Government-operated health care plans and providers have substantially the same obligations as private entities for Privacy Rule compliance purposes. Significantly, federally-run programs have the additional obligation of complying with the Privacy Act of 1974, which restricts the type and amount of information about individuals, including health information, that can be shared with other federal agencies and the public. Federal agencies are still subject to enforcement effort by OCR.

OCR looks at whether the Privacy Rule establishes a government database containing the personal health information of all individuals whose information has been submitted to the government. The Guidance states that the Privacy Rule does not create 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. Furthermore, the Rule does not require a physician or other covered entity to send any medical information to the government and does not expand the government's access to information, except that the Rule provides OCR with the authority to investigate complaints that Privacy Rule rights or protections have been violated.

MISCELLANEOUS FAQs

The Guidance also specifically addresses how individuals can enforce their individual rights, and the relationship between the covered entity and the individual enforcing such rights. For example, to the extent that an individual believes that his or her privacy rights have been violated, the individual may submit a written complaint to OCR within 180 days of the date that the complaining individual knew or should have known that the act had occurred. The 180-day requirement may be waived for good cause.

If a patient requests copies of medical records as provided by the Privacy Rule, the covered entity is permitted to impose reasonable, cost-based fees. The fee may include copying costs, including supplies and labor, and postage if mailing is required. If the individual has agreed to receive a summary of the information, the covered entity may charge a fee for preparation of the summary.

Finally, OCR addresses whether the Rule permits covered entities to fax patient information to another provider's office. OCR observes that the Rule permits physicians to disclose PHI to another covered entity for treatment purposes and that this may be accomplished by fax or other means; provided, however, that there are reasonable and appropriate administrative, technical and physical safeguards to protect the privacy of information that is disclosed (i.e., this is HHS' subtle way of reminding us not to forget the obligations of the Security Regulations, even if they are not yet final).