January 8, 2001

Brief Summary of the HIPAA Privacy Rule

I. Introduction

On December 28, 2000, the Department of Health and Human Services (HHS) published the long, complex, and controversial final rule on health information privacy.[1] The final rule applies to covered entities (*i.e.*, health plans, health care clearinghouses, and most health care providers) with respect to protected health information. The rule also applies indirectly to "business associates" who perform certain functions on behalf of, or provide certain services for, covered entities. The compliance date is February 26, 2003, although small health plans have an additional year to comply.

Congress authorized HHS to issue the rule in the Health Insurance Portability and Accountability Act of 1996 (HIPAA, P.L. 104-191). Under HIPAA, Congress directed HHS to issue a regulation establishing standards with respect to the privacy of individually identifiable information transmitted in connection with the HIPAA standard transactions.[2] HHS was authorized to exercise its authority, however, only if Congress failed to enact privacy legislation with respect to the HIPAA standard transactions within three years -- *i.e.*, by August 21, 1999. Congress did not meet the deadline. In November 1999, HHS issued a controversial proposed rule on health information privacy. The agency received nearly 52,000 comments on its proposal.

The final rule responds to many of these comments but remains contentious. Some believe that HHS has exceeded the agency's statutory authority in the final rule. The health care industry is reviewing the final rule and may ask the new Administration to reduce the rule's burden on industry. Some consumer privacy advocates have asserted that there are gaps in the rule's protections with respect to marketing and sharing of information with law enforcement. Meanwhile, HHS has called upon Congress to enact comprehensive legislation to cover additional entities and strengthen what it describes as "woefully inadequate penalties" for violations of the rule. Although legal challenges to the final rule were widely anticipated before its issuance, we are unaware of any pending litigation. We will closely monitor any developments that impact the implementation of the final rule.

---

[1] 65 Fed. Reg. 82461 (Dec. 28, 2000).

[2] HIPAA required HHS to develop national standards for health plans and health care providers to use when engaging in common electronic health care transactions. Health care clearinghouses may perform translation between standard and non-standard formats. The final HIPAA standard transaction rule, published in August 2000, standardized eight transactions, including health care claims, payment and remittance advice, and coordination of benefits.

II. Major Changes in the Final Rule

There are far too many differences between the proposed and final rule to enumerate here. The following are five major policy differences:

- *PHI covered in any form or medium.* The final rule covers protected health information ("PHI") in any form or medium (*e.g.*, electronically maintained, paper records, oral communications). The proposed rule covered such information only when electronically maintained or transmitted by a covered entity, or when the electronic information took on another form (*e.g.*, computer printout).

- *New consent requirement for direct treatment providers.* Direct treatment providers are now required in most circumstances to obtain consent prior to using or disclosing PHI for treatment, payment, and health care operations. The proposed rule did not require any covered entity to obtain consent or authorization to use or disclose most PHI for treatment, payment, or health care operations.

- *Significant changes to minimum necessary standard.* The final rule retains the "minimum necessary" standard (a principle requiring uses and disclosures to be limited to the minimum amount necessary to accomplish a purpose). However, the final rule applies the minimum necessary standard to many routine uses and disclosures by requiring workforce access controls and standard protocols for disclosure. The proposed rule required individual "minimum necessary" determinations for each use and disclosure.

- *Marketing and fundraising provisions.* The final rule permits certain limited marketing and fundraising without specific authorization. The proposed rule required authorization for such uses and disclosures.

- *Private right of action.* There is no new private right of action under the privacy rule. The proposed rule would have required contracts between business partners and covered entities to make individuals "third party beneficiaries" to the contracts. Many commenters thought that this provision would have created a new right of action under state law. The final rule eliminated this provision. In some states, however, individuals may have a right of action under existing law.

III. Brief Summary

The rule is extraordinarily complex. The brief summary below provides a top-level overview to assist in understanding the structure of the rule.

1. <u>Applicability</u>:

A. *Covered Entities* (§§164.500, 160.103): The rule applies to covered entities with respect to protected health information. Covered entities are health plans, health care clearinghouses, and health care providers who electronically transmit health information in connection with HIPAA

standard transactions. Each type of covered entity is defined in significant detail. Health care clearinghouses are subject to more limited requirements than other covered entities.

B. *Protected Health Information / De-identified Information)* (§§ 164.501, 164.514): PHI is individually identifiable information relating to an individual's health, the provision of health care, or payment for the provision of health care. PHI does not include de-identified information, *i.e.*, information that does not identify an individual. A covered entity, or a business associate (*see below*) of the covered entity, may de-identify PHI (1) by having a person with appropriate knowledge determine that the risk of identifying an individual is very small; or (2) removing a list of 18 identifiers (provided the entity does not have actual knowledge that the de-identified information could be used to identify an individual).

2. **Uses and Disclosures of PHI** (§§ 164.502, 164.514(h)): A covered entity may not use or disclose PHI, except as permitted or required under the rule. The only required disclosures are to an individual (under provisions allowing access to information about that individual and an accounting of disclosures of that information) and to the Secretary of HHS for compliance purposes. Generally, the covered entity must follow verification requirements to ensure that the person requesting PHI is authorized to receive it The following provisions relate to conditions that must be met for permissive uses and disclosures:

A. *Consent* (§164.506): Health care providers that provide direct treatment to individuals generally are required to obtain consent from an individual before using or disclosing PHI to carry out treatment, payment, or health care operations. (Treatment, payment, and health care operations each are defined in great detail.) Treatment may be conditioned on provision of consent. Other covered entities (such as health plans, indirect treatment providers, and health care clearinghouses) are not required to obtain consent for treatment, payment, or health care operations. These other covered entities have the option of obtaining consents and a health plan may condition enrollment on consent.

B. *Authorization* (§164.508): Consent and authorization are different concepts and apply to different situations. Covered entities generally are required to obtain authorization from an individual before using or disclosing PHI (unless consent has been obtained and the use relates to treatment, payment, or health care operations). Authorizations are needed for many uses and disclosures of psychotherapy notes and most research that includes treatment of an individual. Treatment, payment, enrollment in a health plan, or eligibility for benefits generally may not be conditioned on provision of an authorization. Research-related treatment may be conditioned on such an authorization.

C. *Consent or Authorization Not Required* (§164.512): Consent or authorization is not required for certain uses or disclosures of PHI. The listing of permissible uses and disclosures includes: (1) uses and disclosures required by law; (2) uses and disclosures for public health activities; (3) disclosures about victims of abuse, neglect, or domestic violence; (4) uses and disclosures for health oversight activities; (5) disclosures for judicial and administrative proceedings; (6) disclosures for law enforcement purposes; (7) uses and disclosures about decedents; (8) uses and disclosures for cadaveric organ, eye or tissue donation purposes; (9) uses and disclosures for: (A) research purposes, if such research receives a waiver of authorization from an Institutional Review Board (IRB) or a privacy board, or (B) reviews preparatory to research; (10) uses and disclosures to avert a serious threat to health or safety; (11) uses and disclosures for specialized government functions; and (12) disclosures for workers' compensation. Most clinical trials will not fall within the research exception for IRB or privacy board waiver of authorization because the exception applies only where the research cannot practicably be conducted without a waiver.

D. *Marketing and Fundraising* (§§ 164.501, 164.514(e), (f)): "Marketing" is defined to exclude certain activities, such as describing a provider network or services provided by a covered entity or benefit plan. An exception to the authorization requirements applies to certain narrowly defined marketing activities. These marketing activities include face-to-face communications or communications about products or services of nominal value. Additional marketing communications are permitted without authorization for health-related services of a covered entity or a third party if the communication meets certain criteria (*e.g.*, prominently states whether remuneration is received for making the communication) and the individual is instructed how to opt out of future communications. Another limited exception applies to fundraising activities.

E. *Directory Information and Involvement in an Individual's Care:* Generally, a covered entity may use PHI to maintain a facility directory unless the individual objects. After giving an individual the opportunity to agree or object, a covered entity may disclose PHI to a family member, friend, or other identified person if the PHI is directly relevant to such person's involvement in the individual's health care. Special rules allow a covered entity to use judgment if the individual is not present to agree or object to such use (*e.g.*, picking up a prescription from a pharmacy).

3. **Minimum Necessary** (§§164.502(b), 164.514(d)): When using or disclosing PHI or requesting it from another covered entity, a covered entity must make reasonable efforts to limit the use or disclosure to the minimum amount necessary to accomplish the intended purpose. This requirement does not apply to certain limited situations

such as disclosures or requests by a health care provider for treatment or disclosure pursuant to an authorization.

A. *Uses*: With respect to uses of information, the covered entity must identify classes of persons within its workforce that need access to PHI to carry out their duties, and the category of PHI to which access is needed and the conditions appropriate to the access.

B. *Routine Disclosures*: With respect to routine disclosures, the covered entity must implement policies and procedures (which may be standard protocols) that limit PHI to the amount reasonably necessary.

C. *Non-Routine Disclosures*: With respect to non-routine disclosures, a covered entity must develop criteria designed to limit PHI to the amount reasonably necessary and review requests for disclosure on an individual basis in accordance with the criteria.

4. **Business Associates** (§§ 160.103, §164.502(e), 162.504(e)): A business associate is a person (and may be a covered entity itself) who performs functions or activities on behalf of a covered entity involving the use of PHI (*e.g.*, claims processing), or provides enumerated services for a covered entity involving the use of PHI (*e.g.*, consulting services). A covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf if the covered entity obtains satisfactory assurances that the business associate will safeguard the PHI appropriately. These satisfactory assurances must be documented through a written contract that contains required elements. Generally, a business associate may not use or disclose the PHI in a manner that would violate the rule if done by the covered entity. There are exceptions to this requirement for data aggregation services and for certain uses and disclosures for proper management and administration of the business associate.

5. **Organizational Requirements** (§§ 164.500, 164.504): Legally separate entities may designate themselves as a single affiliated covered entity if all of the covered entities designated are under common ownership and control. Affiliated entities that designate themselves as a single covered entity do not need to enter into business associate contracts to share PHI with one another and may use a single notice of privacy practices and consent (*see below*). Entities that combine multiple functions must comply with the standards applicable to each function. A "hybrid entity" -- which performs covered functions but not as its primary purpose -- must establish safeguards to limit the sharing of information between its health care component and the larger entity. Special rules apply to the sharing of information between a group health plan and the sponsor of the plan. Other rules apply to an "organized health care arrangement" in which legally separate entities share information to benefit the common enterprise.

6. **Administrative Requirements** (§164.530): A covered entity must: (1) designate a privacy official and a contact to receive complaints; (2) train its workforce; (3) have appropriate safeguards for protecting PHI; (4) have a process for receiving and documenting complaints; (5) sanction its workforce for breaches; (6) mitigate (to the extent practicable) known harm resulting from violations of its own practices or the rule by itself or a business associate; (7) refrain from intimidating or retaliatory acts in certain situations; (8) not require an individual to waive the right to file a complaint with the Secretary; (9) implement policy and procedures with respect to PHI which are reasonably designed given the entity's size and activities; and (10) maintain required documentation for six years. Certain group health plans are not subject to many of these requirements.

7. **Individual Rights:**

A. *Notice of Privacy Practices* (§§ 164.502(i), 164.520): An individual has a right to notice of the uses and disclosures of PHI that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties. The notice must contain specific elements and be provided within specific timeframes and with specific frequency. Special requirements apply to electronic notices. A covered entity may not use or disclose PHI in a manner inconsistent with its notice. Organized health care arrangements may comply by providing a joint notice.

B. *Rights to Request Restrictions on Information and Confidential Communications* (§§ 164.502(c), 164.502(h), 164.522): An individual may request that a covered entity restrict its uses and disclosures of PHI to carry out treatment, payment, or health care operations. The covered entity is not required to agree the restriction. If, however, a covered entity agrees to the restriction, it is bound by its agreement. A covered health care provider must accommodate reasonable requests by individuals to receive communications of PHI by alternative means or at an alternative location. A health plan must accommodate such reasonable requests if the individual clearly states that disclosure of all or part of the PHI would endanger the individual.

C. *Access of Individuals to Their Own PHI* (§§ 164.504(e)(2)(E), 164.524): With limited exceptions, an individual has the right to inspect and obtain a copy of PHI retained in a designated record set. A covered entity may deny an individual access based on specified grounds. Certain grounds for denial will provide the individual with an opportunity of review by a licensed health care professional designated by the covered entity. Under its business associate contract, a business associate must agree to make PHI available for access purposes.

D. *Amendment of PHI* (§§ 164.504(e)(2)(F), 164.526): An individual has the right to have a covered entity amend PHI or a record about the individual in a designated record. A covered entity may accept or deny the amendment

under certain circumstances. A business associate must agree to make PHI available for amendment and incorporate amendments under its business associate contract.

E. *Accounting of Disclosures* (§§ 164.504(e)(2)(G), 164.528): An individual has the right to receive a retrospective accounting of disclosures of PHI made by a covered entity for a period of six years prior to the date the accounting is requested. Certain disclosures may be omitted from the accounting, such as disclosures for purposes of treatment, payment, and health care operations, and certain disclosures to health oversight agencies and law enforcement officials. Under its business associate contract, a business associate must agree to provide an accounting of disclosures to the covered entity.

8. **Relationship to Other Laws** (§§160.201-160.205): The federal rule is intended to provide the minimum standard of privacy protections, but allow individual states to provide greater protections. Thus, the rule generally preempts only contrary state laws but not more stringent ones. This general rule applies unless the law falls into a limited category of state laws and a request is made to seek an exception from preemption. An "implied repeal" analysis will be used to resolve conflicts between the rule and other federal laws relating to privacy.

9. **Enforcement** (§§160.300-160.312): HIPAA established criminal and civil penalties for violating the rule. Civil penalties are capped at $25,000 for each identical requirement or prohibition that is violated. HHS has broad authority to investigate complaints, conduct compliance reviews, and obtain access to records. The Secretary of HHS has generally delegated her civil enforcement, implementation, and interpretation authority under the rule to the HHS Office for Civil Rights. HHS plans to issue an additional notice of proposed rulemaking on enforcement matters. The Department of Justice may enforce substantial criminal penalties (ranging from a $50,000 fine and a one-year prison term to a $250,000 fine and a ten-year prison term).

10. **Effective Date and Transition** (§§ 164.532, 164.534): The rule becomes effective on February 26, 2001, but covered entities generally are not required to comply with it until February 26, 2003 (small health plans with receipts of less than $5 million have one additional year). Under certain conditions, a covered entity may use or disclose PHI obtained prior to the compliance date in accordance with a consent or authorization that does not comply with the rule. If the covered entity is conducting a research project that includes treatment under such a consent or authorization, the covered entity may use or disclose PHI, whether received before or after the compliance date, in accordance with that consent or authorization.

IV. Impact Analysis

HHS has estimated a ten-year (2003-2012) cost of compliance with the rule of $17.6 billion (or a net present value of $11.8 billion). The most costly aspects of the privacy rule are considered to be the requirement to designate a privacy official and compliance with the minimum necessary standards.

These costs of complying with the privacy rule are estimated to be offset by an estimated net savings of $29.9 billion (or net present value of $19.1 billion) attributable to the HIPAA standard transactions rule. HHS is considering the privacy rule and the HIPAA standard transactions rule together in order to comply with the directive in HIPAA that standards adopted be consistent with the objective of reducing the administrative costs of providing health care." (§1172(b) of the Social Security Act) HHS also asserts that increased confidence in the health system will lead to savings in earlier cancer treatment, early HIV/AIDs detection, early treatment for sexually transmitted diseases, and encouragement to seek mental health treatment.

V. Contacts for Further Information

We are advising a broad range of clients on the HIPAA privacy rule, including providers, business associates of covered entities, and other firms that obtain or use PHI, such as pharmaceutical companies. For further information on the HIPAA privacy rule, please contact:

Ellen Flannery (202.662.5484; eflannery@cov.com)

Marialuisa Gallozzi (202.662.5344; mgallozzi@cov.com)

Erika King (202.662.5165; eking@cov.com)

Bruce Kuhlik (202.662.5348; bkuhlik@cov.com)

Julie Miller (202.622.5147; jsmiller@cov.com)