HEALTH
PRIVACY
PROJECT

INSTITUTE FOR HEALTH CARE
RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

Overview of
HIPAA Privacy Regulation

Currently, there is no comprehensive federal law that protects the privacy of people's medical records. The 1996 Health Insurance Portability and Accountability Act (HIPAA) included legislative/regulatory deadlines in order to fill this significant gap in federal rules. HIPAA provides that if Congress failed to pass a comprehensive health privacy law by August 21, 1999, the Secretary of Health and Human Services is required to issue health privacy regulations.

Despite the introduction of numerous bills, and many hearings over the past three years, Congress failed to pass health privacy legislation and thus triggered the regulatory deadline. On October 29, 1999, the Clinton Administration issued its draft regulations. By the close of the public comment period, the Administration had received over 52,000 comments, more than half of them from consumers and consumer advocates.

The final regulation was released on December 20, 2000. The regulation went into effect on April 14, 2001. There is a two-year implementation period before compliance with the regulation is required.

A copy of the regulation is available at: http://aspe.hhs.gov/admnsimp/.

The following chart summarizes key provisions of the final regulation and provides Health Privacy Project commentary.

Topic	The Final Regulation	Health Privacy Project Comments
Who's Covered	Covered entities include: ♦ *Health Plans* HMOs, health insurers, group health plans including employee welfare benefit plans ♦ *Health Care Clearinghouses* Persons and organizations that translate health information to or from the standard format that will be required for electronic transactions under HIPAA ♦ *Certain Health Care Providers* Those who use computers to transmit health claims information.	Under HIPAA, the Secretary only has the authority to cover these three entities. The regulation, therefore, does not directly apply to many other entities that collect and maintain health information such as employers, life insurers, researchers, and public health officials. *Only Congress can fill these critical gaps.*
What's Covered	Only the use and disclosure of "protected health information" is covered. In order to be considered "protected health information" under the regulations, information must: ♦ Relate to a person's physical or mental health, the provision of health care, or the payment of health care; ♦ Identify, or could be used to identify, the person who is the subject of the information; and ♦ Be created or received by a covered entity. Such information is protected regardless of the format in which it is transmitted or maintained--oral, electronic or paper.	There is some dispute over whether the Secretary has the authority to cover health information that is in any format other than electronic. Practically speaking, covering health information that is maintained or transmitted in *any* medium or format is a sensible move. Limiting coverage to electronically transmitted data would be impractical, unenforceable and would deter covered entities from moving towards electronic health data systems. Even with this improvement, the regulation still fails to cover a large portion of health care information due to statutory limits on the Secretary's authority; namely, identifiable health information *generated by entities not covered* by the regulations such as employers or life insurers. *Only Congress can fill in these critical*

Topic	The Final Regulation	Health Privacy Project Comments
What's Covered (continued)	There are incentives for covered entities to create and use "*de-identified information*," health information which has been stripped of elements that could be used to identify individual subjects.	*gaps.* Encouraging the use of information that does not identify the patient helps ensure that peoples' privacy can be maintained to the maximum extent possible.
Patient Access	♦ Individuals have a right to see and copy their own health information, including documentation of to whom the information has been disclosed. ♦ Individuals are given the right to request amendment or correction of health information that is incorrect or incomplete. ♦ There are limited exceptions to when patients can access their own information such as when such access would endanger the life or safety of any individual.	Currently, there is no federal law granting persons the right to obtain their medical records. Although the majority of states provide patients the right of access to *some* of their medical records, very few do so in a comprehensive fashion. In fact, some states have *no* such statutory right of access. The final regulation, therefore, establishes a significant, new legal right for individuals to see and copy their own health information.
Notice	Health plans and health care providers are required to provide written notice of their privacy practices, including a description of an individual's rights with respect to protected health information (such as the right to inspect and copy health records) and the anticipated uses and disclosures of this information that may be made without the patient's written authorization.	We are pleased that this basic fair information has been adopted in the regulation.

Topic	The Final Regulation	Health Privacy Project Comments
General Rule-Patient permission required	♦ An individual's written permission is required for all uses or disclosures not permitted or required under the privacy regulation. ♦ The regulation uses two different types of written permission: 1. Consents--used for treatment, payment and health care operations; and 2. Authorizations—used for other purposes.	The regulation permits uses and disclosures *without* authorization or consent for *many* purposes. The distinction between consents and authorizations is somewhat confusing. Consents and authorizations are discussed separately below.
Treatment, Payment, and Health Care Operations **(Consents)**	♦ Covered **health care providers *must*** generally obtain the patient's consent prior to using or disclosing protected health information to carry out treatment, payment, or health care operations. ♦ Providers ***may condition*** treatment on patient's providing consent form. ♦ **Health plans** and **health care clearinghouses *may*** obtain such consent for their own use or disclosure to carry out these purposes. ♦ Health plans ***may condition*** enrollment on provision of consent. ♦ Individuals have a ***right to request restrictions*** on how health information is used or	We believe that obtaining consent before the use or disclosure of health information is a fundamental component of fair information practices. As such, we support the new consent requirement. We are concerned that a consent for treatment will allow uses and disclosures well beyond what the average health consumer would anticipate. Most people would expect that they are consenting only to the use of health information for *their own* treatment. However, under the regulation, such a consent would also permit the provider to use and disclose one patient's health information for the treatment of *other* patients. The right to request a restriction affords individuals with especially sensitive medical conditions an additional

Topic	The Final Regulation	Health Privacy Project Comments
Treatment, Payment, and Health Care Operations (continued)	disclosed for treatment, payment or health care operations purposes.	opportunity to exercise control over their health information. This right should be strengthened.
Authorizations	♦ Authorizations are used for purposes other than treatment, payment and health care operations when use or disclosure is not otherwise permitted in the regulation. ♦ Providers generally *may not* condition treatment on authorization. ♦ Health plans *may* condition enrollment, eligibility and payment on authorization permitting disclosure and use related to these purposes. Psychotherapy notes are an exception.	Patient authorization is critical to protecting patient privacy. Authorizations provide individuals with some degree of control over what information about them is disclosed, to whom, and for what purposes.
Patient Permission *Not Required*	Health information may be disclosed for a number of purposes without any patient authorization or consent including, but not limited to: public health activities, research, and fraud investigations.	See our comments on law enforcement and research.
Business Associates	♦ Business associates are persons who perform functions or activities involving the use or disclosure of protected health information for or on behalf of a covered entity. ♦ A written contract is necessary in order for a business associate to receive information from, or	This requirement indirectly expands the scope of the privacy regulation. Wrongful disclosures that violate business partner contracts may be subject to lawsuits brought by the

Topic	The Final Regulation	Health Privacy Project Comments
Business Associates (continued)	on behalf of, a covered entity. Under the contract, the business associate is essentially bound to the use and disclosure limitations of the regulations.	individual under state contract law. Although we support this indirect regulation of secondary users of health information, we would prefer that these entities be directly regulated. *Only Congress can remedy this situation*.
Minimum Necessary	Covered entities must make reasonable efforts to limit protected health information to the ***minimum amount necessary*** to accomplish the intended purpose of the use, disclosure or request for health information from another. This standard does *not* apply to disclosures for treatment and other specified purposes.	The minimum necessary standard imposes an important limitation on the amount of health information disclosed. However, we believe the standard should apply to a broader category of disclosures, including those made for treatment.
Directory Assistance and Next of Kin	For providing information to a ***directory*** (such as a hospital's patient directory) or to ***next of kin*** or other persons involved in the care of the patient, the patient must be given ***notice*** and the opportunity to ***opt out before*** the information is disclosed.	An **opt in** procedure, where privacy is protected unless the patient agrees to the disclosure, would be preferable.
Psychotherapy Notes	♦ There are stricter requirements than for other health information. Written authorization is required for most uses or disclosures. ♦ Health plans may not condition enrollment or eligibility for benefits on the patient's providing an authorization for the use and disclosure of	Psychotherapy notes differ considerably from other kinds of information in a patient's medical record. Such notes are highly subjective and sensitive, and should not be made available beyond the treating provider without the patient's consent. Notes of psychotherapy sessions are not necessary for health plans to make enrollment, eligibility and payment

Topic	The Final Regulation	Health Privacy Project Comments
Psychotherapy Notes (continued)	psychotherapy notes.	decisions. The approach taken by the regulation is reasonable-- it allows health plans to condition these services on the patient's authorizing the disclosure of treatment times, general diagnosis and other general information but prohibits plans from requiring access to detailed session notes.
Minors' Rights	Unemancipated minor has sole right to exercise rights under regulation including: ♦ Minor has consented to health care service and no other ♦ consent to such health care is required by law; or ♦ Parent or guardian assents to an agreement of confidentiality.	Under this provision, the federal privacy right will attach to the right to consent to treatment. Other law, including state law, will govern when a minor may consent to treatment without adult involvement. Parental notification laws are not affected by the federal regulation.
Law Enforcement	Covered entities are permitted to disclose protected health information to law enforcement officials: ♦ Pursuant to warrant, subpoena, or order issued by a judicial officer; ♦ Pursuant to a grand jury subpoena; or ♦ Pursuant to an administrative subpoena or summons, civil investigative demand or similar certification where a three-part test is met: the information is relevant, the request is specific, and de-identified information could not reasonably be used.	The regulation falls far short of the standards established in most federal privacy laws. Only the first category requires any independent judicial review. Administrative summons and subpoenas may be issued by the investigating authority *with no independent review* by a neutral magistrate to determine whether the request should be granted or denied.

Topic	The Final Regulation	Health Privacy Project Comments
Law Enforcement (continued)	The regulation also permits additional disclosures without any written request.	
Research	Covered entities can disclose protected health information without a patient's authorization only to researchers whose protocol has been reviewed and approved by an Institutional Review Board (IRB) or a "privacy board." The regulation includes new evaluation criteria for all waivers of informed consent. Information can only be released to researchers if it meets the criteria.	Currently, only research *that receives federal funding* is subject to the "Common Rule," a federal regulation that requires that any use of identifiable private information be overseen by an Institutional Review Board (IRB). The final privacy regulation takes an important step forward by extending the Common Rule's requirements for a waiver of informed consent to *all researchers*, including privately funded researchers.
Enforcement	HIPAA grants the Secretary the authority to impose civil monetary penalties against covered entities that fail to comply and criminal penalties for certain wrongful disclosures of protected health information. ♦ The civil fines are capped at $25,000 for each calendar year for each provision that is violated. ♦ The criminal penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain. The maximum is 10 years in prison and a $250,000 penalty ♦ The Secretary will, to the extent practicable, seek the	Of concern is that HIPAA does not provide for a private right of action for individuals, which would allow individuals to sue for violations of their rights. The Administration is on record supporting a private right of action in pending legislation. *Only Congress, however, can give people a right to this critical enforcement mechanism*.

Topic	The Final Regulation	Health Privacy Project Comments
Enforcement (continued)	cooperation of covered entities in obtaining compliance. Any person who believes that a covered entity is not complying with the regulatory requirements may file a complaint with the Secretary.	
Preemption	HIPAA provides that state laws that are more protective of individual privacy will stand. States are also free to pass stronger laws in the future.	Leaving stronger state laws in place is critical. Although most states do not have comprehensive health privacy laws, many states do have detailed, stringent standards for certain information, such as mental health, genetic testing, and HIV/AIDS. These stronger privacy protections would remain in force.