SUMMARY OF HIPAA REGULATIONS

The Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). 1 The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

STATUTORY & REGULATORY BACKGROUND

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to ublicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the Administrative Simplification provisions. HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within OCR Privacy Rule Summary 2 Last Revised 05/03 three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000. In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.3 A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E on the OCR

WHO IS COVERED BY THE PRIVACY RULE

The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the “covered entities”). Health Plans. Individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations (“HMOs”), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies).

**Health Care Providers**. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule. Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all “providers of services” (e.g., institutional providers such as hospitals) and “providers of medical or health services” (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

**Health Care Clearinghouses.** Health care clearinghouses are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.

WHAT INFORMATION IS PROTECTED

**Protected Health Information**. The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."12 OCR Privacy Rule Summary 4 Last Revised 05/03 “Individually identifiable health information” is information, including demographic data, that relates to: the individual’s past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.13 Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

GENERAL PRINCIPLE FOR USES AND DISCLOSURES

Basic Principle. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected heath information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing. Required Disclosures. A covered entity must disclose protected health information in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.17 See OCR “Government Access” Guidance.

PERMITTED USES AND DISCLOSURERS

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual’s authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.18 Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

AUTHORIZED USES AND DISLCOSURES

Authorization. A covered entity must obtain the individual’s written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.44 A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.45 An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. Examples of disclosures that would require an individual’s authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes. All authorizations must be in plain language, and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data. The Privacy Rule contains transition provisions applicable to authorizations and other express legal permissions obtained prior to April 14, 2003.

LIMITING USES AND DISCLOSURES TO THE MINIMUM NECESSARY

Minimum Necessary. A central aspect of the Privacy Rule is the principle of “minimum necessary” use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.50 A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

NOTICE AND OTHER INDIVIDUAL RIGHTS

Privacy Practices Notice. Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The Privacy Rule requires that the notice contain certain elements. The notice must describe the ways in which the covered entity may use and disclose protected health information. The notice must state the covered entity’s duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. The notice must describe individuals’ rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated. The notice must include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their notices. The Rule also contains specific distribution requirements for direct treatment providers, all other health care providers, and health plans.

ADMINISTRATIVE REQUIREMENTS

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity’s business, as well as the covered entity’s size and resources. Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.64 Privacy Personnel. A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity’s privacy practices.

ORGANIZATIONAL OPTIONS

The Rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy protections. Hybrid Entity. The Privacy Rule permits a covered entity that is a single legal entity and that conducts both covered and non-covered functions to elect to be a “hybrid entity.”

Affiliated Covered Entity. Legally separate covered entities that are affiliated by common ownership or control may designate themselves (including their health care components) as a single covered entity for Privacy Rule compliance.

Organized Health Care Arrangement. The Privacy Rule identifies relationships in which participating covered entities share protected health information to manage and benefit their common enterprise as “organized health care arrangements

Covered Entities With Multiple Covered Functions. A covered entity that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions

Group Health Plan disclosures to Plan Sponsors. A group health plan and the health insurer or HMO offered by the plan may disclose the following protected health information to the “plan sponsor”—the employer, union, or other employee organization that sponsors and maintains the group health plan

OTHER PROVISIONS: PERSONAL REPRESENTATIVES AND MINORS

Personal Representatives. The Privacy Rule requires a covered entity to treat a "personal representative" the same as the individual, with respect to uses and disclosures of the individual’s protected health information, as well as the individual’s rights under the Rule.84 A personal representative is a person legally authorized to make health care decisions on an individual’s behalf or to act for a deceased individual or the estate. The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

STATE LAW

Preemption. In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.85 “Contrary” means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.86 The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits.

ENFORCEMENT AND PENALTIES FOR NONCOMPLIANCE

Compliance. Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule.87 The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews. Civil Money Penalties. HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.88 That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

COMPLIANCE DATES

Compliance Schedule. All covered entities, except “small health plans,” must be compliant with the Privacy Rule by April 14, 2003.90 Small health plans, however, have until April 14, 2004 to comply. Small Health Plans. A health plan with annual receipts of not more than $5 million is a small health plan.91 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 Code of Federal Regulations (CFR) 121.104 to calculate annual receipts. Health plans that do not report receipts to the Internal Revenue Service (IRS), for example, group health plans regulated by the Employee Retirement Income Security Act 1974 (ERISA) that are exempt from filing income tax returns, should use proxy measures to determine their annual receipts