

**HIPAA'S PRIVACY REGULATIONS
AND THEIR IMPACT ON GROUP HEALTH PLANS**

ALI-ABA Video Law Review

Health Plans, HIPAA and COBRA Update

April 27, 2006

Prepared by:

**Greta E. Cowart, Esq.
Haynes and Boone, LLP
901 Main Street, Suite 3100
Dallas, TX 75202-3789
214.651.5000**

Updated March 10, 2006

TABLE OF CONTENTS

	Page ¹
I. Protection of Individually Identifiable Information	1
A. To Whom Do The Privacy Regulations Apply?	2
B. Definitions.....	2
1. Group Health Plan.....	2
2. Health Care	4
3. Health Care Clearinghouse	4
4. Health Information.....	4
5. Health Plan.....	4
6. Trading Partner Agreement.....	5
7. Business Associate.....	5
8. Payment is Defined	6
9. What is Protected Health Information?.....	7
10. Summary Health Information	7
11. Health Care Provider.....	7
12. Health Care Operations.....	8
13. Organized Health Care Arrangement.....	8
14. Hybrid Entity.....	9
C. Modifications	9
D. Different Entities Recognized.....	9
1. What is the Entity?.....	9
2. Hybrid Entities	9
3. Affiliated Entities.....	11
4. Covered Entities with Multiple Functions	11
E. State Law Preemption/Interaction.....	11
1. HIPAA vs. State Law.....	11
2. ERISA Preemption and Privacy.....	14
a. Under ERISA	14
b. Preemption and State Causes of Action.....	14
F. Complaints/Compliance.....	21
G. Overview of Requirements	22
1. Health Care Clearinghouse Rules	23
2. Group Health Plan Rules	24
3. Health Care Providers	24
4. How Much is Disclosed or When Does Minimally Necessary Not Apply?.....	24
5. Individuals May Request Restrictions on Uses and Disclosures	25
H. Some Standards Vary by Type of Covered Entity	25

¹ Internal Pagination.

II.	Uses and Disclosures of PHI Addressed in Regulation – Permitted Disclosures	26
A.	General Rules for Permitted Disclosures	26
B.	Disclosures to the Individual or the Secretary of HHS	27
C.	Permitted Uses and Disclosures of De-Identified Information	27
D.	Permitted Disclosure or Use of a Limited Data Set	27
1.	Limited Data Set Defined	28
2.	Limited Data Set Agreement Standards	28
3.	Consequence of Pattern of Violations	29
E.	Permitted Disclosure to Business Associates	29
1.	Business Associate Agreement Standards	31
F.	Permitted Disclosure Regarding Deceased Individuals	33
G.	Permitted Disclosures to Personal Representatives	33
H.	Other Permitted Disclosures	34
1.	Disclosure by Work Force/Business Associate on Good Faith Belief of Violation	34
2.	Disclosures to Law Enforcement Regarding Suspected Perpetrators of Criminal Acts	35
I.	Permitted Uses and Disclosures by a Group Health Plan	35
1.	Special Requirements for Group Health Plans	36
2.	Plan Document Requirements	36
3.	Separation between Group Health Plan and Plan Sponsor	37
J.	Permitted Use or Disclosure for Treatment, Payment or Health Care Operations by a Health Care Provider	38
III.	Uses or Disclosures for Which Authorization is Required	39
A.	Use or Disclosure of Psychotherapy Notes	39
B.	Authorization for Marketing	40
C.	Combination of Authorization for Disclosure or Use with Notice	41
D.	Standards for a Valid Authorization	42
IV.	Use or Disclosure with Opportunity to Agree or Object	43
A.	Facility Directories	43
B.	Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes	44
C.	Uses and Disclosures When the Individual is Present	44
D.	Use and Disclosure When the Individual is Not Present	44
E.	Use and Disclosures for Disaster Relief	44
V.	Uses and Disclosures for Which No Authorization or Opportunity to Agree or Object is Required	45
A.	Uses and Disclosures	45
B.	Disclosures for Public Health Activities	45
C.	Disclosures Regarding Victims of Abuse, Neglect or Domestic Violence	47
D.	Disclosures for Health Oversight Activities	48

E.	Disclosures for a Judicial and Administrative Proceedings.....	48
F.	Disclosures for Law Enforcement Purposes	49
1.	Disclosures Required by Law	49
2.	Disclosure Pursuant to Order, Warrant, Subpoena, etc.....	49
3.	Disclosures of Limited Information for Identification and Location Purposes	50
4.	Disclosures Regarding Victims or Suspected Victims of Crimes.....	50
5.	Decedents.....	50
6.	Crime on the Premises	50
7.	Reporting Crime in Emergencies.....	51
G.	Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes ..	51
H.	Uses and Disclosures for Research Purposes.....	51
I.	Use or Disclosure to Avert a Serious Threat to Health or Safety	51
J.	Uses and Disclosures for Specialized Governmental Functions.....	52
1.	Correctional Institution	52
2.	Governmental or Public Health Benefits	53
3.	Workers Compensation.....	53
K.	Uses and Disclosures for Fundraising.....	54
L.	Uses and Disclosures for Underwriting and Related Purposes.....	54
VI.	Other Requirements Relating to Uses and Disclosures	54
A.	De-Identified Protected Health Information	54
B.	Uses and Disclosures of Protected Health Information for Marketing.....	55
VII.	Disclosures in Litigation.....	55
A.	General Guidelines.....	55
B.	Pursuant to an Order of a Court or Administrative Proceeding.....	56
C.	Responding to Subpoenas, Discovery Requests or Other Lawful Processes That Are Not Accompanied by an Order of a Court or Administrative Tribunal.....	56
VIII.	New Disclosure Procedures and Restrictions	57
A.	General Standards Minimum Necessary - Access Limited Within Covered Entity.....	57
B.	Verification Must Be Made Before Disclosure.....	59
IX.	New Notice and Administrative Procedure Requirements Under the Privacy Regulations	59
A.	Notice of Privacy Practices for Protected Health Information.....	59
1.	Self Insured or Partially Self Insured Plans	59
2.	Fully Insured Group Health Plan or HMO and Plan Receives More Than Summary Health Information	59
3.	Fully Insured or HMO and Protected Information Only Received in Summary Format or Not at All	60

4.	Correctional Institution Plans	60
B.	Notice Contents.....	61
C.	Individuals May Request Restrictions on Access	63
D.	Access to the Individual.....	63
E.	Right to Amend.....	64
F.	Right to Accounting of Disclosures	65
G.	Confidential Communications	66
H.	Procedures to be Implemented by Covered Entities	67
I.	Effective Date	68
J.	Transition Rule for Authorizations	69
X.	Enforcement of Privacy for Individually Identifiable Health Information.....	69
A.	Criminal Enforcement.....	69
B.	Civil Enforcement.....	70
C.	No Private Cause of Action	71
XI.	Security	71
XII.	Privacy in Mergers, Acquisitions and Corporate Transactions.....	71
A.	Due Diligence	71
B.	Plan Transition Issues	73

HIPAA'S PRIVACY REGULATIONS AS FINALLY MODIFIED AND THEIR IMPACT ON GROUP HEALTH PLANS

CAVEAT: This outline summarizes the HIPAA Privacy Regulations as modified. No one should rely on this as legal advice. In every situation, the application of the rules requires careful analysis by an attorney who is familiar with your particular situation.

- I. Protection of Individually Identifiable Information. Act § 262 and 42 U.S.C. §§ 1171 through 1179 require the Secretary of Health and Human Services ("Secretary of HHS") to adopt standards for health plan information data and for protection of individually identified information. Proposed standards were published on November 3, 1999.¹ Proposed standards for the security of individually identifiable health information and for electronic signatures were published on August 12, 1998.² The National Committee on Vital and Health Statistics published their comments on the Proposed standards on July 10, 2000.³

The final standards for electronic transactions were published on August 17, 2000 with an effective date of October 16, 2000.⁴ Modifications to the final electronic claims standards were published on May 31, 2002, modifying the standards for retail pharmacy transactions for claims, encounters and coordination of benefits.⁵ This outline does not address the standards for electronic transactions. The final regulations on the standards for privacy of individually identifiable health information were published on December 28, 2000.⁶ The final regulations were similar to the original regulations in many ways.

The Administrative Simplification Compliance Act was enacted on December 27, 2001, permitting covered entities to apply for approval to extend the compliance deadline for the electronic transaction. The Administrative Simplification Compliance Act also clarified that it did not extend the effective date for the Privacy Regulations and in fact codified the effective date for the privacy regulations.⁷ A minor modification to the final privacy regulations was published on December 29, 2000.⁸ On March 27, 2002, proposed modifications to the final regulations were published which predominantly changed provisions related to health care providers and made other limited changes.⁹ On August 14,

¹ 64 F.R. 59917.

² 63 F.R. 43241 (1998).

³ 65 F.R. 42370 (2000).

⁴ 45 C.F.R. § 152.900 (2000).

⁵ 67 F.R. 38044 (2002).

⁶ 65 F.R. 82461 (2000).

⁷ P.L. 107-105 (2001).

⁸ 65 F.R. 82944 (2000).

⁹ 67 F.R. 14776 (2002).

2002, final modification to the privacy regulations were issued incorporating many of the changes in the March 27, 2002 modifications and some additional modifications.¹⁰ This outline looks at the privacy regulations as modified by the August 14, 2002 final modifications, and after the changes in the Final Security Regulations issued on February 20, 2003. The Final Security Regulations are addressed in a separate paper.

The Constitutionality of the privacy regulations was challenged in litigation. The challenge questioned whether they exceeded the legislative scope of the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”), and whether the privacy regulations violated the 1st, 4th and 10th Amendments to the Constitution was upheld.¹¹

A. To Whom Do The Privacy Regulations Apply? The privacy regulations apply to health plans, health care clearinghouses, and health care providers who transmits any health information in electronic form in connection with a transaction that is covered by the provisions in Subchapter C of the Subtitle A of Title 45 of the Code of Federal Regulations.¹² Thus, health care providers who submit claims only in paper form are not required to comply. The privacy regulations apply to the covered entities, health plans, health care clearinghouses, and health care providers who transmit health information in electronic format, and to others with whom such covered entities contract to provide certain services, and to the Secretary of Health and Human Services and others engaged on his behalf in ascertaining the compliance of the covered entities and the enforcement of the applicable requirements.¹³

B. Definitions. The final regulations include more expanded definitions. The definitions contained in both Part 160 and Part 164 are treated as having the same meanings.¹⁴

1. Group Health Plan. A group health plan is defined by the regulations to include an employee welfare benefit plan as defined in section 3(1) of the Employee Retirement Income Security Act of 1974, including both insured and self insured plans to the extent that the plan provides medical care, including items and services that are paid for as medical care to employees and their dependents provided that the plan has 50 or more participants or is administered by an entity other than the employer that established the plan.¹⁵

¹⁰ 67 F.R. 53181 (2002).

¹¹ *The Association of American Physicians & Surgeons, Inc. v. U.S. Department of Health and Human Services, Inc.*, 67 Fed. Appx. 253 (5th Cir. 2003), *aff'g* 274 F. Supp.2d 1115 (S.D. Tx. June 17, 2002); *South Carolina Medical Association v. Thompson*, ____ U.S. ____, 2003 U.S. LEXIS 8010, U.S. No. 03-114, *cert. denied* Nov. 3, 2003, 327 F.3d 346 (4th Cir. 2003).

¹² 45 C.F.R. § 160.102 (2000).

¹³ 45 C.F.R. § 160.301 (2000).

¹⁴ 45 C.F.R. § 160.302 (2000).

¹⁵ 45 C.F.R. § 160.103 (2000). This exception operates to exclude health flexible spending accounts maintained by a

The group health plan definition also refers to the health plan definition in the regulations described below. The extent to which a group health plan must comply varies by the type of group health plan, its funding and the type of information it receives, protected health information, summary health information or individually identifiable health information. The privacy regulations do not apply to certain excepted benefits listed in section 2791(c)(1) of the Public Health Service Act which include only:

- a. coverage only for accident or disability income insurance, or any combination thereof,
- b. coverage issued as a supplement to liability insurance,
- c. liability insurance and automobile liability insurance,
- d. workers compensation or similar insurance,¹⁶
- e. automobile medical payment insurance,
- f. credit only insurance,
- g. coverage for on-site clinics, and
- h. other similar insurance coverage specified in regulations under which benefits for medical care are secondary or incidental to other insurance benefits.¹⁷

A health plan also does not include a plan that provides health care benefits directly or through insurance, reimbursement or otherwise that has fewer than 50 participants and that is self administered.¹⁸ The fewer than 50 participants and self administered exception was designed to cover a small employer's self-administered health flexible spending account plan. It is not clear if the workers' compensation and similar insurance exception extends to the Texas workers' compensation opt-out ERISA self-insured plans. Other states have statutorily based self-insured workers' compensation plans which do not opt-

small employer (<50 employees) if the employer administers the plan itself.

¹⁶ In Texas, if an employer is not required to maintain workers' compensation, the employer may elect to not obtain coverage under § 406.002 of the Texas Labor Code and become a non-subscriber. Non-subscribers provide similar benefits under ERISA plans. These plans provide reimbursement for medical care and would be subject to the HIPAA privacy regulations as ERISA plans since they are commonly established as ERISA plans and are outside of the workers' compensation system in Texas.

¹⁷ 45 C.F.R. § 160.103 (2000) health plan definition.

¹⁸ See group health plan definition in 45 C.F.R. § 160.103 (2000).

out, but act as substitutes for workers' compensation and those are arguably within the exception.

2. Health Care. Health care includes care of services and supplies related to the health of the individual including preventative, diagnostic, therapeutic, rehabilitative, maintenance, palliative care, and counseling, service assessment or procedures with respect to physical or mental condition, functional status of an individual or the effects of structure or function of the body, and also the sale or dispensing of any drug device, equipment or other item in accordance with the prescription.¹⁹
3. Health Care Clearinghouse. A health care clearinghouse is a public or a private entity including a billing service, repricing company, a community health management information system or community health information system, and value added networks that either (1) processes or facilitates the processing of health information received from another entity in a non-standard form containing non-standard data content or non-standard data elements into a standard transaction, or (2) receives standard transaction from another entity and processes or facilitates the processing of information into a non-standard format or non-standard data content for the receiving entity.²⁰
4. Health Information. The health information that is protected by the final regulations includes not only the electronic information, but also includes any information whether oral or recorded in any form or medium that is created and received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present or future physical or mental health condition of the individual, the provision of health care to the individual or the past, present or future payment for the provision of health care to the individual.²¹ Thus, the definition is broad enough to cover all information submitted with a health plan claim or appeal of a denied claim.
5. Health Plan. The regulation adds a definition for health plan to include both an individual or a group plan that provides or pays for the cost of medical care and includes either singly or in combination a group health plan, a health insurance issuer, an HMO, Part A or Part B of Medicare (and in 2006 Part D), the Medicaid program, the issuer of a Medicare supplemental policy, the issuer of long term care policy, an employee welfare benefit plan or any other arrangement established or maintained for the purpose of offering or providing health benefits to employees of two or more employers (the

¹⁹ 45 C.F.R. § 160.103 (2000).

²⁰ 45 C.F.R. § 160.103 (2000).

²¹ 45 C.F.R. § 160.103 (2000).

multiemployer plans), a health care program for active military personnel, veterans health care program, the civilian health and medical program of the Uniformed Services (CHAMPUS), the Indian Health Service program, the federal employees health benefit program, an approved state child health plan, the Medicare Plus Choice program (now the Medicare Advantage program), a high risk pool maintained by a state or under state law, and any other individual or group plan that provides or pays for the cost of medical care. However, a health plan does not include any policy, plan or program to the extent it provides or pays for the cost of excepted benefits as provided under § 2971(c)(1) of the Public Health Service Act (the HIPAA excepted benefits enumerated in I.B.1. above), any government funded program, its principal purpose is providing or paying for the cost of health care, or whose principal activity is the direct provision of health care, or the making of grants to fund the direct provision of health care to persons.²² A small health plan is a health plan that has annual receipts of \$5,000,000 or less.²³ A group health plan for an employer of fewer than 50 participants that administers its own claims will also not be defined as a group health plan for purposes of the privacy regulations.²⁴

6. Trading Partner Agreement. The final regulations incorporate the concept of trading partner agreement. A trading partner agreement is used in the final regulations for providing the standardized data codes that were published on August 17, 2000.²⁵ In this case the trading partner agreement is any agreement related to the exchange of information in electronic transactions whether the agreement is a separate and distinct agreement or part of a larger agreement between the parties. A transaction is the transmission of information between two parties related to health care, including claims or equivalent encounter information, payment, remittance, coordination of benefits, claim status, enrollment, disenrollment, eligibility, premium payment, referral, certification, authorization, first report of injury, health claim attachments, and any other transaction covered by the regulations.
7. Business Associate. A group health plan or health care provider often enters into arrangements with business associates regarding providing services that involve the handling of protected health information. For example, a self insured group health plan will contract with a claims administrator to adjudicate its claims, retain a attorney for advice on legal issues and claim disputes, or retain the services of a computer system technician to work on a system with group health plan information in it. Each of those service

²² See health plan definition in 45 C.F.R. § 160.103 (2000).

²³ 45 C.F.R. § 160.102 (2000).

²⁴ 45 C.F.R. § 160.103 (2000).

²⁵ 45 C.F.R. § 162.915 (2000).

providers are business associates of the plan. The final regulations define a business associate as a person who on behalf of the covered entity (or an organized health care arrangement in which the covered entity participates), performs or assists in the performance of the following in a capacity other than as an employee or member of the work force of such entity: (1) a function or activity involving use or disclosure of individually identifiable health information including claims processing or administration; data analysis processing or administration; utilization review; quality assurance; billing; benefit management; practice management or repricing; or (2) any other function or activity regulated by the privacy regulations; or (3) that provides (other than in the capacity as a member of the work force of the covered entity) legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such entity; or (4) a service that involves a disclosure of individually identifiable health information from the covered entity or arrangement or from another business associate of a covered entity or arrangement. A covered entity that participates in an organized health care arrangement who performs a function or activity described above for or on behalf of an organized health care arrangement, or provides a service described above does not simply through the performance of such function or activity and the provision of such service become a business associate of the covered entity included in the organized health care arrangement. A covered entity can also be a business associate of another covered entity (e.g., a health care clearinghouse could be a business associate of a health plan or health care provider to convert claims to or from the standard format).²⁶

8. Payment is Defined. The final regulations have defined payment to include activities undertaken (1) by a health plan to obtain premiums, to determine or fulfill its responsibilities for coverage or provision of benefits under the health plan, or (2) by a health care provider or a health plan to obtain or provide the reimbursement for provision of health care, that relates to individuals to whom health care is provided, and (3) includes, but is not limited to, determinations of eligibility or coverage and adjudication or subrogation of health benefit claims, risk adjusting amounts due based on enrollees health status and demographic characteristics, billing, claims management, collection activities, obtaining payment under a contract for the insurance and related health care data processing, review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges, utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services, and disclosure to consumer

²⁶ 45 C.F.R. § 160.103 (2000); OCR Guidance Explaining Significant Aspects of Privacy Rule, Business Associates, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

reporting agencies of any of the following protected health information relating to collection of premiums or reimbursements, including name and address, date of birth, social security number, payment history, account number, name and address of the health care provider and/or health plan, all constitute payment activities.²⁷

9. What is Protected Health Information? The final regulations defined protected health information as individually identifiable health information that is (1) transmitted by electronic media, (2) maintained in any medium described in the definition of electronic media in § 162.103 of the Subchapter, or (3) transmitted or maintained in any other form or medium. Protected health information does exclude individually identifiable health information included in education records under 20 U.S.C. § 1232g (education records available to parents), or records described in 20 U.S.C. § 1232(g)(A)(4)(B)(iv) (education records for those over age 18 or in college) and in employment records.²⁸ Thus, health information need not ever be transmitted electronically in order to be protected by the privacy regulations.²⁹ Protected health information does not include employment records held by a covered entity in its role as employer.³⁰ Employment records need to be segregated from health plan records since the health plan is a covered entity subject to the privacy regulations and the employment records are not protected health information because they are not created or received by a covered entity, unless the employer is a covered entity.
10. Summary Health Information. Summary health information is information that may be derived from individually identifiable health information and that summarizes claims history, claims expenses, types of claims experience by individuals under a health plan and which has been de-identified in compliance with the standards except that the de-identification with respect to individuals may include a five digit zip code level as opposed to a three digit zip code level and it excludes name and social security number.³¹
11. Health Care Provider. A health care provider is a provider of services (as defined in section 1861(u) of the Social Security Act (42 U.S.C. § 1395x(u))), a provider of medical or health services (as defined in § 1861(s) of the Social Security Act or 42 U.S.C. § 1395x(s)) and any other person or organization

²⁷ 45 C.F.R. § 164.501 (2000).

²⁸ 45 C.F.R. § 160.103 (2003).

²⁹ 45 C.F.R. § 160.103 (2003).

³⁰ 45 C.F.R. § 160.103, protected health information definition (2)(iii) (2003); and 67 F.R. 53182, 53191 (2002).

³¹ 45 C.F.R. § 164.504(a) (2000).

who furnishes, bills or is paid for health care in the normal course of business.³²

12. Health Care Operations. Health care operations include (a) quality assessment and improvement activities, including outcomes evaluation, development of clinical guidelines as long as obtaining generalizable knowledge is not the primary purpose of the studies resulting from the activities, population based activities related to improving health or reducing health care costs, protocol development, (b) case management, care coordination and contacting of health care providers and patients with information about treatment alternatives and related functions that do not include treatment, reviewing the competence or qualification of health care professionals in evaluating practitioners and providing health plan performance information and conducting training programs in which students, trainees or practitioners in areas of health care learn about supervision, practice or improve their skills as health care providers and in training non-health professionals, accreditation, certification, licensing or credentialing activities, (c) underwriting or premium writing and other activities related to the creation, renewal and replacement of contract of health insurance or health benefits, and, ceding or securing or placing the contract for reinsurance risk related to claims for health care, (d) conducting or arranging for medical review, legal services, auditing functions, including fraud and abuse detection and compliance programs, (e) business planning and development, (f) business management, and (g) general administrative activities of the entity, including management activities related to implementation and compliance, customer service, resolution of internal grievances, and the sale, transfer, merger or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity, and the due diligence related to such merger of covered entities activity, and creating de-identified health information and fund-raising for the benefit of a covered entity.³³
13. Organized Health Care Arrangement. An organized health care arrangement is (a) a clinically integrated health care setting where individuals typically receive health care from more than one health care provider, (b) an organized system of health care in which more than one covered entity participates and in which the entities hold themselves out to the public as participating in a joint arrangement and the entities participate in joint activities that include utilization review, quality assessment or payment activities (e.g., a multidisciplinary clinic with various out patient therapy centers), or (c) a group health plan and a health insurance issuer or HMO with respect to the

³² 45 C.F.R. § 160.103 (2000).

³³ 45 C.F.R. § 164.501 and § 164.502 (2000) and 45 C.F.R. § 164.501 (2002).

group health plan, but only with respect to the protected health information created or received by the issuer or HMO that relates to participants or beneficiaries in the group health plan, or (d) a group health plan and one or more group health plans, each of which are maintained by the same plan sponsor.³⁴ For example, an HMO or insurer that provides benefits under a group health plan is part of an organized health care arrangement.³⁵ Another example would be a health flexible spending account plan with 50 or more employees and a group health plan sponsored by the same employer.

14. Hybrid Entity. A hybrid entity is a single legal entity that is a covered entity, whose business activities include both covered and non-covered functions, provided that it designates the health care components as required in the privacy regulations.³⁶

C. Modifications. The final regulations cannot be modified more frequently than once every 12 months.³⁷ The effective date of any modifications cannot be earlier than 180 days after the effective date of the final rule in which the Secretary of HHS adopts the modification.³⁸ The final modifications were published on August 14, 2002, and are effective no sooner than 60 days after publication, or October 15, 2002, therefore they will be effective at the same time as the final regulations on April 14, 2003 or 2004 depending on the size of the plan.³⁹

D. Different Entities Recognized.

1. What is the Entity? The final regulations define whether an entity is subject to the regulation in total or in part, by looking at organizational requirements and defines common control as an entity that has power, directly or indirectly, to significantly influence the actions or policies of another entity. The final regulations find common ownership exists if an entity or entities possess ownership or equity interest of 5% or more in another entity.⁴⁰

2. Hybrid Entities. The final regulations recognize that a hybrid entity is a single legal entity that is a covered entity; whose business activities include both covered and non-covered functions; and that designates health care

³⁴ 45 C.F.R. § 160.103 (2003).

³⁵ OCR Guidance Explaining Significant Aspects of Privacy Rule, Business Associates, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

³⁶ 45 C.F.R. § 164.103 (2003).

³⁷ 45 C.F.R. § 160.104(a) (2000).

³⁸ 45 C.F.R. § 160.104 (2000).

³⁹ 67 F.R. 53181 (2002).

⁴⁰ 45 C.F.R. § 164.103 (2003).

components in accordance with Reg. § 164.105(a)(2)(iii)(C). A health care component is a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(C).⁴¹ For example, a large discount store that includes a pharmacy and an optometrist would be a hybrid entity and could designate that the pharmacy and optometrist are the health care components subject to HIPAA privacy.

If an entity is a hybrid entity (covering both functions covered by the privacy regulations and functions not covered), then the final regulations' reference to a covered entity only refers to the health care component of the covered entity provided the covered entity designates the health care components and documents the designation in compliance with § 164.530(j). The designation must include any component that would be a covered entity if it were a separate legal entity. A component may either perform covered functions or activities that would make it a business associate if the component that performs covered functions were a separate entity.⁴² An entity that includes more components than just the health care component must ensure that the health care component complies with the privacy regulations and must ensure that it does not disclose protected health information to another component of the entity that would be prohibited from receiving information. The components designated must be separate and distinct and must not use or disclose protected health information that is created or received by the component for the purpose of the entities' activities that are not the health care activities. Any individual who works for both the health care component and another part of the entity must not use or disclose information that it receives in the course of its work in the health care component in violation of the regulations. The hybrid entity must make sure all components, including a component that would be a business associate if it were a separate entity, do not use or disclose the protected health information violation of the regulations.⁴³

An entity is responsible for designating itself as a single covered entity. If all of the covered entities are under common control, an entity may designate itself as a single entity. Any designation of the single entity must be documented and the documentation must be maintained in a written or electronic record.⁴⁴

⁴¹ 45 C.F.R. § 164.103 (2003).

⁴² 45 C.F.R. § 164.103 (2003); 45 C.F.R. § 164.105(a) (2003).

⁴³ 45 C.F.R. § 164.105(a)(2)(ii) (2003).

⁴⁴ 45 C.F.R. § 164.105(b) (2003).

A wrap around plan that includes non-health welfare benefits and health benefits could treat itself as a hybrid entity and designate the portions of the plan that are health care components subject to the privacy regulations and those portions which are not health care components.⁴⁵ The health care component may not disclose protected health information to non-health care components, e.g., the health plan may not provide protected health information to the life insurance or disability insurance benefits or vendors.⁴⁶

3. Affiliated Entities. Any affiliated covered entity must ensure that its use of any protected health information complies with the requirements. If the designation as an affiliated entity combines the functions of health plan, health care provider or health care clearinghouse, then the entity must comply with the standards for an entity with multiple covered functions under 45 C.F.R. § 164.504(g).⁴⁷
4. Covered Entities with Multiple Functions. If a covered entity has multiple covered functions then the covered entity must comply with the standards and requirements and implementation specifications applicable to the health plan, health care provider or health care clearinghouse function being performed. Thus, the requirements apply based upon the function being performed. A covered entity that performs multiple functions can use or disclose the protected health information of individuals who received the covered entity's health plan or health care provider services, but not both, only for the purposes related to the appropriate function performed with respect to such individual.⁴⁸ For example, a wrap around health plan covering multiple benefits may try to segregate privacy health plan functions out separately in the plan documents and its privacy provisions and notices, or it could spin off the non-health plan pieces into a separate plan to isolate those from the privacy requirements or designate itself as a hybrid entity and designate its health care components subject to the privacy requirements.⁴⁹

E. State Law Preemption/Interaction.

1. HIPAA vs. State Law. The final regulations include a section on the preemption of state law and define a state law as being contrary when it is impossible to carry out both the state and federal requirements, or if the state law stands as an obstacle to the accomplishment of the execution of the full

⁴⁵ 45 C.F.R. § 164.105(a) (2003).

⁴⁶ 45 C.F.R. § 164.105(a)(2)(ii)(A) – (C) (2003).

⁴⁷ 45 C.F.R. § 164.105(b) (2003).

⁴⁸ 45 C.F.R. § 164.504(g) (2000).

⁴⁹ 45 C.F.R. § 164.105(a) (2003).

purposes and objectives of the privacy regulations.⁵⁰ The final regulations also define a more stringent a state law as a law that meets one or more of the following criteria: (1) it prohibits or restricts a use or disclosure in circumstances under which the use or disclosure would otherwise be permitted by the privacy regulations except if a disclosure is required by the Secretary of HHS in connection with determining whether one of the covered entities is in compliance with the privacy regulations or the disclosure is to the individual who is the subject of the individually identifiable health information;⁵¹ (2) it permits greater rights of access or amendment to the individual who is subject to the individually identifiable health information than permitted by the privacy regulations; (3) the law is also more stringent if it is with respect to information to be provided to the individual who is the subject of the individually identifiable health information about a use, a disclosure, rights or remedies, and it provides a greater amount of information; (4) the law is more stringent with respect to the form, substance or need for express legal permission from an individual who is the subject of the individually identified health information for use or disclosure of any individual identifiable health information if it provides the requirements that narrow the scope, duration or increase the privacy protections afforded or reduces the coercive effect of the circumstances surrounding the express legal permission; (5) the law is more stringent with respect to record keeping or other requirements relating to accounting for disclosures if it provides for the retention or the reporting of more detailed information or for a longer duration than the six years provided by the privacy regulations; or (6) it provides greater privacy protection for the individual.⁵²

As a general rule, a standard, requirement or implementation specification under the final privacy regulations that is contrary to the provision of state law preempts the provision of state law, except if one or more of the following conditions is met: (1) a determination is made by the Secretary of HHS that the state law provision is necessary (a) to prevent fraud and abuse, (b) to ensure appropriate state regulation of insurance in health plans to the extent it is expressly authorized by state statute or regulation, (c) for state reporting on health care delivery or costs, or (d) for the purpose of serving a compelling need related to public health safety or welfare; (2) if its principal purpose is regulating the manufacture, registration, distribution, dispensing or other control of any controlled substance or anything that is deemed to constitute a controlled substance by state law; (3) the state law relates to the privacy of health information is more stringent than the privacy standards in the final regulations; (4) the state law provides for the reporting of a disease

⁵⁰ 45 C.F.R. § 160.202 (2000).

⁵¹ 45 C.F.R. § 160.202 (2000).

⁵² 45 C.F.R. § 160.202 (2000); 45 C.F.R. § 164.524, § 164.526 and § 164.528 (2000).

or injury, child abuse, birth or death, or for the conduct of public health surveillance and investigation or intervention; or (5) the state law requires the health plan to report or provide access to information for the purpose of management of financial audits or program monitoring and evaluation or the licensing or certification of facilities or individuals.⁵³

Some state laws have been tested. In a medical malpractice dispute the defendant's counsel had ex parte pre-trial communications with plaintiff's treating physician and plaintiff objected that such communications constituted a violation of HIPAA. The Maryland Law did not prohibit such communications. The Maryland Confidentiality of Medical Records Act ("MCMRA") and its mandate on disclosure was raised by the defense as permitting the ex parte communication when a patient had sued the health care provider. The court found the MCMRA was not more stringent than HIPAA because with respect to the form, substance or need for express legal permission from the individual who is the subject the MCMRA did not provide requirements narrowing the scope or duration, increasing the privacy protections, or reducing the coercive effect of the circumstances surrounding the express legal permission, nor did it provide greater privacy protection for the individual and the MCMRA did not give the individuals more control over their medical records. The court stated the key component in analyzing HIPAA's more stringent requirement is "the ability of the patient to withhold permission and to effectively block disclosure."⁵⁴

In order to request an exception for a state law, requests must be made by a state through its chief elected official or its designee. The exception must be requested through the Secretary of HHS.⁵⁵ The Secretary of HHS makes the determination of whether an exception to the privacy regulations remains in effect. Any exception for state law only remains in effect until either the state law or federal standard is materially changed so that the ground for the exception no longer exists, or the Secretary revokes the exception.⁵⁶ See also the discussion herein of the regulatory provisions compared to state laws. Additional cases have considered whether HIPAA privacy preempts a certain state law with a variety of results.⁵⁷

⁵³ 45 C.F.R. § 160.203 (2000).

⁵⁴ *Law v. Zuckerman*, 2004 U.S. Dist. LEXIS 3755 (S.D. D. Md. 2004).

⁵⁵ 45 C.F.R. § 160.204 (2000).

⁵⁶ 45 C.F.R. § 160.205 (2000).

⁵⁷ *National Abortion Federation v. Ashcroft*, 2004 (U.S. Dist. LEXIS 4530 (S.D.N.Y. 2004)); *Planned Parenthood Federation of America, Inc. v. Ashcroft*, 2004 U.S. Dist. LEXIS 3383 (N.D. Ca. 2004); *Northwestern Memorial Hospital v. Ashcroft*, 2004 U.S. App. LEXIS 5724 (7th Cir. 2004); *Law v. Zuckerman*, 2004 U.S. Dist. LEXIS 3755 (D. Md. 2004); *Patient Advocates, LLC v. Prysuka*, 2004 U.S. Dist. LEXIS 682 (D. Me. 2004); *A Helping Hand, LLC v. Baltimore County, Maryland*, 295 F. Supp.2d 585 (D. Md. 2003); *Hutton v. City of Martinez*, 2003 U.S. Dist. LEXIS

2. ERISA Preemption and Privacy. Another consideration for group health plans will be whether the laws will be preempted under ERISA since the plan will be required to incorporate privacy provisions. Recent case law developments in ERISA preemption did not find sufficient conflict and viewed insurance law requirements as part of plan design when a divided court determined that a state law on claims review procedures requiring an independent reviewer was not preempted.⁵⁸

Further, one court found that state medical privacy laws were not preempted by ERISA when an employer obtained medical information on an employee and used it to terminate the employee, which use was found to be outside the employer's functions as plan administrator or a fiduciary to the plan.⁵⁹ Thus, questions exist regarding whether the state medical privacy laws will be preempted either by ERISA or under HIPAA's preemption language.

- a. Under ERISA.

The incorporation of the privacy provisions in the plan document as required by the Privacy Regulations,⁶⁰ provides the participants the right to seek to enforce the terms of the plan document under section 502(a)(3) of ERISA. However, the remedy for seeking to enforce the plan's terms is limited to appropriate equitable relief. Courts are still determining what constitutes appropriate equitable relief following *Great-West Life & Annuity Ins. Co. v. Knudson*.⁶¹

- b. Preemption and State Causes of Action.

After Congress enacted the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),⁶² Congress was given 36 months in which to enact legislation protecting the privacy of individually identifiable health information. When Congress failed to act within the 36 month period, the U.S. Department of Health and Human Services was required to promulgate final regulations on the privacy of individually identifiable health information. While

19852 (N.D. Ca. 2003); *U.S. v. The Louisiana Clinic*, 2002 U.S. Dist. LEXIS 24062 (E.D. La. 2002); and *Croskey v. BMW of North America, Inc.*, 2005 U.S. Dist. LEXIS 3673 (E.D. Mich. 2005).

⁵⁸ *Rush Prudential HMO, Inc. v. Moran*, 122 S. Ct. 2151 (2002).

⁵⁹ *Darcangelo v. Verizon Communications, Incorporated*, 292 F.3d 181 (2002).

⁶⁰ 45 C.F.R. § 164.504(f) (2003).

⁶¹ 534 U.S. 204, 112 S. Ct. 708, 151 L.Ed.2d 634 (2002).

⁶² Pub. L. No. 104-191 (August 21, 1996).

Congress did not enact any legislation, many states did enact legislation establishing statutes creating private rights and causes of actions for violations in medical privacy. Many states also recognize causes of action in case law for intentional infliction of emotional distress in tort when a tortfeasor either intentionally or recklessly did some act which caused emotional distress. However, this is often difficult to prove without extreme or outrageous conduct.⁶³ The majority of states have recognized a common law invasion of privacy tort for publicity given to private life if something private is made public by communicating it to the public at large.⁶⁴

HIPAA also contained a number of provisions dealing with preemption. The first provision was contained in Title I, Part A, Group Market Reforms, Subpart 3, Exclusion of Plans, Enforcement and Preemption in Section 2723 of HIPAA which stated with respect to continued preemption with respect to group health plans:

Nothing in this part shall be construed to affect or modify the provisions of section 514 of the Employee Retirement Income Security Act of 1974 with respect to group health plans.⁶⁵

This "part" refers to the provision included in the Public Health Service Act dealing with the applicable portability, access and renewability requirements that apply to health insurance issuers under the Public Health Service Act. Part A of HIPAA under Title I did not include the statutory provision with respect to the privacy of individually identifiable health information.⁶⁶

The next provision addressing ERISA preemption under HIPAA was contained in section 2746 of the Public Health Service Act under Part B of Subtitle B of Title I of HIPAA. This provision in section 2746(b) states that:

Nothing in this part (or part C insofar as it applies to this part) shall be construed to affect or modify the

⁶³ *Thornburg v. Federal Express Corp.*, 62 S.W.3d 421, 428 (Mo. App. 2002).

⁶⁴ *Doe v. Methodist Hosp.*, 690 N.E.2d 681 (Ind. 1997); Restatement (Second) of Torts § 652D; *Beaumont v. Brown*, 257 N.W.2d 522 (Mich. 1977); *State of Montana Board of Dentistry v. Kandarian*, 886 P.2d 954 (Mont. 1995); *Y.G. and L.G. v. The Jewish Hospital of St. Louis*, 795 S.W.2d 488 (Mo. 1990).

⁶⁵ 42 U.S.C. 300gg-23.

⁶⁶ 42 U.S.C. 300gg-23.

provisions of section 514 of the Employee Retirement
Income Security Act of 1974 (29 U.S.C. § 1144).⁶⁷

Part B and Part C which are referred to in this section deal with guaranteed availability of individual health insurance, guaranteed renewability of health insurance coverage, certification of coverage, state flexibility in the individual market reform and enforcement of the portability rules in the individual market rules. Subtitle C dealt with health coverage availability studies, reports on Medicare reimbursement of telemedicine, allowing federally qualified HMOs to offer high deductible plans, volunteer services provided by health professionals at free clinics and some findings and severability provisions. These were not the parts which contained the provisions authorizing the promulgation of the privacy regulations.

The privacy provisions were enacted under Title II of HIPAA which deals with prevention of health care fraud and abuse, administrative simplification and medical liability reform. The privacy provisions were contained in section 264 in Title II. There are two references to ERISA within Title II – one contained in section 250 describing the relationship of the Subtitle dealing with criminal laws to ERISA authority. Section 250 stated, "Nothing in this subtitle shall be construed as affecting the authority of the Secretary of Labor under section 506(b) of ERISA with respect to violations of Title 18, United States Code."⁶⁸ This is with respect to criminal prosecutions dealing with health care fraud offenses.

The second provision that dealt with preemption in Title II was contained in section 264(c), the section enabling issuance of the privacy regulation. In this case, the provision for preemption with respect to privacy under Part C of Subtitle F indicated that a regulation promulgated as the result of the statute on the privacy of individually identifiable health information, "shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards or implementations specifications that are more stringent than the requirements, standards or implementations specifications imposed under the regulations."⁶⁹ There are no other provisions within Title II of HIPAA that explicitly provide ERISA preemption protection, or that indicate they are not intended to alter

⁶⁷ 42 U.S.C. 300gg-46.

⁶⁸ 29 U.S.C. 1136 and Pub. L. No. 104-191, section 250.

⁶⁹ Compare sections 250 and 264 of Title II to sections 102 and 111 of Title I of Pub. L. No. 104-191.

the ERISA preemption as the provisions under Title I of HIPAA provided.

Thus, there is nothing in the HIPAA statute which indicates that the privacy regulations were not intended to alter or were intended to follow the standard ERISA preemption analysis. Since the statute in several places noted that it was not to alter the normal ERISA preemption analysis, but did not also include that language in the provisions dealing with the privacy medical information, it would appear that either Congress may have intended to omit such broader protection or did not consider the impact of the regulations on ERISA plans.

Even though commenters requested that there be clarification regarding the scope of preemption under ERISA, the U.S. Department of Health and Human Services ("HHS") refused to issue any regulations to belief that they had no authority to address such issue when they issued the final regulations.⁷⁰ The U.S. Department of Health and Human Services ("HHS") indicated it had no authority to issue regulations under ERISA.⁷¹ The preamble to the final regulations issued on December 28, 2000, responded to a comment in which the commenter wanted clarification that ERISA preempts all state laws (including those relating to the privacy of individually identifiable health information to permit multi-state employers to use a set of rules to administer their plans).⁷² The preamble's response to a comment regarding "ERISA" and the "more stringent" or "contrary" definition and their application to an ERISA plan implied that the more stringent and contrary definitions standards would apply to ERISA plans as well as non-ERISA plans. A further concern expressed regarding ERISA plans, which are not now subject to certain state laws because of field preemption provisions of ERISA, is that these will become subject to state privacy laws that are "more stringent" than the federal requirements due to the operation of section 1178(a)(2)(B), together with section 264(c)(2).⁷³ HHS's response to such concern was:

While the courts will have the final say on these questions, it is argued that these sections simply leave in place more stringent state laws that would

⁷⁰ 65 F.R. 82462, 594 (2000).

⁷¹ *Id.*

⁷² 65 F.R. 82461, 82594 (2000).

⁷³ 65 F.R. 82582 (2000).

otherwise apply; to the extent that such state laws do not apply to ERISA plans because they are preempted by ERISA, we do not think that the section 264(c)(2) overcomes the preemption effected by section 514(a) of ERISA.⁷⁴

Thus HHS recognizes that the courts will have the final say and indicates that it is HHS's view that sections simply leave in place more stringent state laws that would otherwise apply. To the concern that those state laws do not apply to ERISA plans because they are preempted by ERISA, HHS did not state that the statutory reference in section 264(c)(2) of HIPAA overcomes the preemption effected by section 514(a) of ERISA, nor did it state that ERISA preemption should preclude application of all state laws. This impacts the HIPAA privacy right notice disclosures.

However, the concern remains that there are state laws which will be more stringent, and that may apply or may be drafted in ways that they will apply to not only health plans but to other entities or persons in a manner that they will not be preempted when reviewed by a court. HHS referred in the preamble to the final regulations to the preamble of the proposed regulations wherein it stated:

However, section 514(b) of ERISA, 29 U.S.C. 1144(b)(2)(A) expressly excepted from preemption state laws which regulate insurance. Section 514(b)(2)(B) of ERISA, 29 U.S.C. 1144(b)(2)(B), provides that an ERISA plan is deemed not to be an insurer for purposes of regulating the plan under state insurance laws. Thus, under the deemer clause, States may not treat ERISA plans as insurers subject to direct regulation by State law. Finally, section 514(d) of ERISA, 29 U.S.C. 1144(d), provides that ERISA does not "alter, amend, modify, and validate, impair or supersede any law of the United States."

We considered whether the preemption provisions of section 264(c)(2) of Pub. L. No. 104-191, discussed in the preceding section would give effect to state laws that would otherwise be preempted by section 514(a) of ERISA. Our reading of the statutes together is that the effect of section 264(c)(2) is simply to leave in

⁷⁴ 65 F.R. 82462, 82582 (2000).

place State privacy protections that would otherwise apply which are more stringent than federal privacy protections. In the case of ERISA plans, however, if those laws are preempted by section 514(a), they would not otherwise apply. We do not think that it is the intent of section 264(c)(2) to give an effect to State law that would not otherwise have in the absence of subsection 264(c)(2). Thus, we would not view the preemption provisions below as applying to State laws otherwise preempted by section 514(a) of ERISA . . . to date our discussions and consultations have not uncovered any particular ERISA requirement that would conflict with the rules proposed below.⁷⁵

Thus, the concern becomes if such State statutes are drafted in such a way that they will not be preempted under conflict preemption under section 514(a) of ERISA or complete preemption under section 502(a) of ERISA there may be a state law that will survive ERISA preemption and each must be analyzed under ERISA's preemption analysis. This means each state law must be reviewed under both ERISA preemption analysis and if the statute survives such analysis, then under HIPAA privacy preemption analysis.

It is important to remember that some State laws have not been preempted and in recent years the scope of preemption has been addressed and limited by the Supreme Court a number of times. In 1995, the Court addressed a tax imposed on health care services paid for by non-insured plans and stated:

In sum, cost-uniformity was almost certainly not an object of preemption, just as laws with only an indirect economic effect on the relative cost of various health insurance packages in a given state are a far cry from those "conflicting directives" from which Congress meant to insulate ERISA plans. See 498 U.S. at 142. Such state laws leave plan administrators right where they would be in any case, with the responsibility to choose the best overall coverage for the money. We therefore conclude that such state laws do not bear the requisite "connection with" ERISA plans to trigger preemption.⁷⁶

⁷⁵ 64 F.R. 59917, 60001 (1999).

⁷⁶ *New York State Conference of Blue Cross Blue Shield Plans v. The Travelers Insurance Company*, 514 U.S. 645, 662

The "connection with" test was considered again, two years later, when New York's tax was again before the Court. In this case the Court stated:

The HFA is a tax on hospitals. Most hospitals are not owned or operated by ERISA funds. This particular ERISA fund has arranged to provide medical benefits for its plan beneficiaries by running hospitals directly, rather than by purchasing the same services at independently run hospitals. If the fund had made the other choice, and had purchased health care services from a hospital, that facility would have passed the expense of the HFA onto the fund and supplying beneficiaries through the rates it set for the services provided. The fund would then have had to decide whether to cover a more limited range of services for its beneficiaries, or perhaps to charge its plan members higher rates. Though the tax in such a circumstance would be "indirect," its impact on the fund's decisions would be in all relevant respects identical to the "direct" impact felt here. Thus, the supposed difference between direct and indirect impact-upon which the Court of Appeals relied in distinguishing this case from *Travelers*⁷⁷-cannot withstand scrutiny. Any state tax, or other law, that increases the cost of providing benefits to covered employees will have the same effect on the administration of ERISA plans, but that simply cannot mean that every state law with such an effect is preempted by the federal statute.⁷⁸

Furthermore, the court has chiseled further away at what constitutes a law that is preempted by finding that in the *Kentucky Association of Health Plans, Inc. v. Miller*,⁷⁹ finding that any willing provider statutes regulate insurance even though they specifically were originally directed toward and cover insured plans as well as self-insured plans. In this case the Court found that, "it suffices that they substantially affect the risk pooling arrangement between the insurer

(1995).

⁷⁷ 514 U.S. 645 (1995).

⁷⁸ *DeBuono v. NYSA-ILA Medical and Clinical Services Fund*, 520 U.S. 806, 816 (1997).

⁷⁹ 538 U.S. ____ (2003).

and the insured." In this case the Court not only adopted new standards to determine whether or not the law regulated insurance, it permitted a law that applied both to self-insured non-ERISA plans, HMOs and insurers, but it also applied to any health benefit plan that included chiropractic benefits to request to include any licensed chiropractor who agreed to apply by the rules to serve as a participating provider.⁸⁰

While there may be a question of whether the state laws protecting medical privacy will apply, there is still a second question under section 502 of ERISA which deals with what remedy would exist. Under ERISA section 502, the Supreme Court has stated that the civil enforcement provisions contained in section 502 were modeled to be the exclusive remedy provided and found that there was a clear expression of Congressional intent that ERISA's civil enforcement scheme would be exclusive. Thus, any cause of action under state law which attempted to create a new remedy would be preempted.⁸¹ Thus, a participant would be left seeking to enforce their rights under any state law or for violation of the privacy provisions in the plan requesting appropriate equitable relief or to enforce the plan under sections 502(a)(1)(B) or 502(a)(2) for appropriate relief under section 409 for a breach of fiduciary duty or under section 502(a)(3) to enjoin any act which violates any provision of the plan, or to obtain other appropriate equitable relief or to enforce the terms of the plan. Thus, any relief sought would be placing the individual back in the inquiry that exists following the *Great-West Life & Annuity Ins. Co. v. Knudson*⁸² in attempting to determine what is appropriate equitable relief.

Due to the interaction of the ERISA preemption analysis and the more carefully drafted State laws, a medical plan's compliance with HIPAA's privacy regulations should be carefully reviewed to ascertain if potential deficiencies may exist which could expose the plan to risks.

- F. Complaints/Compliance. Any person who believes that one of the covered entities is not complying may file a complaint with the Secretary of HHS. The complaints must be filed in writing either on paper or electronically and must name the entity that is

⁸⁰ 538 U.S. ____ (2003).

⁸¹ *Pilot Life Ins. Co. v. Dedeaux*, 481 U.S. 41 (1987); however, note that some administrative appeals provided by state law for insured plans have been upheld. *Rush Prudential HMO, Inc. v. Moran*, 536 U.S. 355 (2002), and *Unum Life Ins. Co. of America v. Ward*, 526 U.S. 358 (1998).

⁸² 534 U.S. 204 (2002).

the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements. Any complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of had occurred.⁸³ The Secretary is authorized to perform compliance reviews and to require entities to make disclosures in order to determine whether the entities are complying.⁸⁴

The HIPAA privacy regulations and statute do not create a private right of action, but only permit enforcement by the Secretary of the Department of Health and Human Services.⁸⁵

- G. Overview of Requirements. The final regulation requires group health plans to develop procedures for handling the privacy of individually identifiable health information, and also requires them to incorporate not only procedures, but provisions within the plan document governing the special limitations on how the standards apply to certain group health plans that are either fully insured or fully insured through an HMO with varies depending on whether or not the entity receives health information in more than a summary format.⁸⁶

The procedures must include compliance with the disclosure requirements that require the plan to notify individuals regarding their privacy procedures as well as their privacy rights.⁸⁷ There are requirements to make an accounting of all disclosures of protected health information, upon request, excluding certain disclosures of information used for treatment and payment of health care operations or disclosure to the individuals who are the subject of the protected information.⁸⁸ The privacy regulations include in the implementation specification requirements for what provisions and procedures must be included in the plan documents and in contracts with business associates.⁸⁹ The final security regulations also include business associate agreement requirements.⁹⁰ A privacy officer must be appointed

⁸³ 45 C.F.R. § 160.306 (2000).

⁸⁴ 45 C.F.R. § 160.310 (2000).

⁸⁵ *Slue v. New York University Medical Center*, 409 F. Supp. 2d 349 (S.D. N.Y. 2006); *Runkle v. Gonzalez*, 2005 U.S. Dist. LEXIS 22219 (D.O.C. 2005); *Protection & Advocacy System, Inc. v. Freudenthal*, 2006 U.S. Dist. LEXIS 3529 (D. Wyo. 2006); *Redtke v. American Federation of State, County and Municipal Employees – Milwaukee District Council 48*, 376 F. Supp. 2d 893 (E.D. Wis. 2005); *Haranzo v. The Department of Rehabilitative Services*, 2005 U.S. Dist. LEXIS 27302 (W.D. Va. 2005); *Johnson v. Milwaukee County*, 2006 U.S. Dist. LEXIS 6892 (E.D. Wis. 2006); See X. below.

⁸⁶ 45 C.F.R. § 164.530 (2000).

⁸⁷ 45 C.F.R. § 164.520 (2000).

⁸⁸ 45 C.F.R. § 164.528 (2000).

⁸⁹ 45 C.F.R. § 164.504(e) and (f) (2000).

⁹⁰ 45 C.F.R. § 164.314(a) (2003).

and personnel must be trained on privacy requirements.⁹¹ The training requirement is an ongoing requirement. The final regulations require covered health care providers to provide a privacy notice and may require a group health plan to provide privacy procedures and notifications to the participants in the group health plan. The extent and content of the notice depends on how the group health plan is funded and the extent to which the group health plan receives health information on individuals and the form of such information.⁹²

The privacy regulations apply to covered entities, health plans, health care clearinghouses and health care providers who transmit health information in an electronic form in a standard transaction.⁹³ As part of the compliance requirements the covered entities must also comply with the other provisions of Parts 160 and 162 of the regulations under Title 45 and Subtitle A, Subchapter C. These include the standards for electronic transactions.⁹⁴

Generally a health plan or health care provider or health care clearinghouse may not use or disclose an individual's individually identifiable health information, except as permitted or required by the privacy regulations. Permitted uses and disclosures will be enumerated below. There are also uses and disclosures that are required by law and uses and disclosures that can occur with the consent, authorization or with giving an individual an opportunity to object or agree. Each covered entity must keep records of the information it receives and any requests for amendments or disclosures of individually identifiable health information for a period of six years. An accounting of the disclosures and amendments must be made upon request of the individual.⁹⁵

1. Health Care Clearinghouse Rules. The requirements for the privacy of individually identifiable health information generally applies to all of the entities.⁹⁶ However a health care clearinghouse must comply with certain standards or requirements on implementation, standards or specifications when it is creating or receiving health care information as a business associate of another covered entity. In such situations, it must comply with the requirements for any uses and disclosure of any protected health information under 45 C.F.R. § 164.502, the requirements under § 164.504 relating to organizational requirements for covered entities, including

⁹¹ 45 C.F.R. § 164.530(a) and (b) (2000).

⁹² 45 C.F.R. § 164.520 (2000).

⁹³ 45 C.F.R. § 164.104 (2000).

⁹⁴ 45 C.F.R. §§ 160.101-104 and 162.100-1802 (2000), and §§ 162.900, 162.920, 162.1002, 162.1103, 162.1202, 162.1302, 162.1402, 162.1502, 162.1602, 162.1702, and 162.1802 as modified on February 20, 2003.

⁹⁵ 45 C.F.R. § 164.530(j)(2) (2000) and 45 C.F.R. § 164.528 (2000).

⁹⁶ 45 C.F.R. § 164.500(a) (2000).

designation of the health care components of a covered entity, and § 164.512 relating to use and disclosure for which authorization or an opportunity to agree or object is required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information. It must comply with the transition requirements and the compliance dates for the implementation of the privacy standards. If a health care clearinghouse receives or creates protected health information other than as a business associate of a covered entity, it must comply with all of the standards and implementation specifications. The standards do not apply to the Department of Defense or any federal agency and non-governmental organization acting on its behalf in providing health care to overseas foreign national beneficiaries.⁹⁷

2. Group Health Plan Rules. The privacy requirements impact a group health plan differently depending upon how it is funded and what type of information the plan receives.⁹⁸ The group health plan must determine to which requirements it is subject under the privacy regulations and must understand the rules for uses and disclosures. The group health plan will be required to comply with all applicable implementation standards, e.g., business associate agreement standards.
3. Health Care Providers. Health care providers that transmit claims electronically in the standardized transaction format must fully understand the permitted uses and disclosures and the restrictions related thereto. Health care providers must understand all applicable implementation standards, including providing the notice, training its staff, and all other administrative requirements.
4. How Much is Disclosed or When Does Minimally Necessary Not Apply? As a general rule, any use or disclosure of the protected health information must be limited by the covered entity to the minimum necessary to accomplish the intended purpose of the disclosure use or request. Minimum necessary policies and procedures must limit who within the entity has access to personal health information based on job responsibilities and the nature of the business.⁹⁹ However, the minimum necessary restriction on the amount of the disclosure does not apply to (1) the disclosures to or requests by health care providers for treatment, (2) use or disclosure made to the individual as

⁹⁷ 45 C.F.R. § 164.500(b) and (c) (2000).

⁹⁸ See 45 C.F.R. § 164.520 and § 164.530 (2000) for notice and administrative requirement that apply to group health plans.

⁹⁹ OCR Guidance Explaining Significant Aspects of Privacy Rule, Minimum Necessary, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

permitted or as required when the individual requests it, (3) any use or disclosure for which an authorization by the individual is required under § 164.508 (psycho therapy notes or pursuant to a valid authorization), except the minimum necessary standard still will apply for any use or disclosure when it is requested by a covered entity for its own use or disclosure, (4) disclosures made to the secretary of HHS for compliance reviews purposes; (5) a use or disclosure that the covered entity is required by law to make; (6) disclosures or uses that are required for compliance with applicable requirements of the privacy regulations, or (7) uses or disclosures in compliance with the electronic standard for transactions.¹⁰⁰ Disclosures or uses in the electronic standard include those elements required or situationally required; however, the minimally necessary standard does apply to information included in the transaction date as optional elements.¹⁰¹

5. Individuals May Request Restrictions on Uses and Disclosures. If a covered entity agrees to a restriction on the use or disclosure of protected health information with the individual as permitted under the regulations, the covered entity may not use or disclose the information in violation of the restriction.¹⁰² A covered entity is not required to agree to a requested restriction on use or disclosure, unless it is a request for Confidential Communication as discussed in IX.G. below.

- H. Some Standards Vary by Type of Covered Entity. A covered health plan or health care provider must comply with the standards for confidential communications when it is communicating protected health information.¹⁰³ There are two slight variations on the standards – one for health care providers and one for health plans. The covered entity is required to have a notice describing the uses and disclosures it may make of protected health information that is consistent with its policies.¹⁰⁴ The requirements for providing the notice vary depending on the type of entity and for a group health plan depending upon how the health plan is funded and the extent to which it receives health information in a manner other than a summary format.¹⁰⁵

¹⁰⁰ *Id.*

¹⁰¹ 45 C.F.R. § 164.502(b) (2002); OCR Guidance Explaining Significant Aspects of Privacy Rule, Minimum Necessary, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

¹⁰² 45 C.F.R. § 164.502(c) (2000).

¹⁰³ 45 C.F.R. § 164.502(h) and § 164.522(b) (2000).

¹⁰⁴ 45 C.F.R. § 164.502(i) (2000); see 45 C.F.R. § 164.520 (2000) for determining who must maintain a notice and who has the obligation to provide the privacy practices notice.

¹⁰⁵ 45 C.F.R. § 164.520 (2000).

II. Uses and Disclosures of PHI Addressed in Regulation – Permitted Disclosures.

A. General Rules for Permitted Disclosures. The general rule is the covered entity may not use or disclose protected health information except (a) a disclosure to the individual himself, (b) a disclosure for treatment, payment or health care operations as permitted under 45 C.F.R. § 164.506 (2000), (c) incident to a use or disclosure that is otherwise permitted or required by the HIPAA privacy regulations; provided, the covered entity has complied with the applicable requirements of the minimum necessary standard, and minimum necessary implementation standard, and the standard on safeguards, (d) pursuant to and in compliance with an authorization, (e) pursuant to an agreement or as permitted by the provision governing disclosures with an opportunity to agree or object, or (f) as permitted by and in compliance with the provisions governing uses or disclosures for which an authorization or an opportunity to agree or object is not required, for disclosure of limited data sets, disclosures for fund-raising, disclosures for underwriting and related purposes, disclosure of de-identified information, disclosures by whistleblowers or work force members who are victims of crimes, or which are consistent with the covered entity's notice of privacy practices.¹⁰⁶

1. Incidental disclosures are permitted as long as the covered entity has implemented reasonable safeguards and implements the minimum necessary standard. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as the result of another use or disclosure that is permitted by the privacy regulations. However, the covered entity must have appropriate administrative technical and physical safeguards that protect against uses and disclosures not permitted as well as that limit incidental uses or disclosures. Reasonable safeguards will vary from one covered entity to another depending on factors such as the size of the entity and nature of its business.¹⁰⁷
2. Some reasonable safeguards are described in the Guidance issued Dec. 4, 2002, speaking quietly while discussing a patient's condition with family members in a public area, avoiding using patient's names in hallways, using physically isolated or locking file cabinets or records rooms for storage of protected health information or by providing additional security such as passwords or computers maintaining personal information.¹⁰⁸

¹⁰⁶ 45 C.F.R. § 164.502(a) (2000).

¹⁰⁷ OCR Guidance Explaining Significant Aspects of Privacy Rule, Incidental Uses and Disclosures, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

¹⁰⁸ *Id.*

3. A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.¹⁰⁹
 4. The covered entity must maintain role based access policies that limit which members of its work force have access to protected health information for treatment, payment and health care operations based on those who need access to perform their jobs.¹¹⁰
- B. Disclosures to the Individual or to the Secretary of HHS. Covered entities are generally required to disclose information to an individual when the individual requests his/her own information pursuant to the requirements for access by the individual to the protected health information and for the accounting of any disclosure or when required by the Secretary of HHS to investigate or determine the covered entity's compliance with the privacy regulations.¹¹¹
- C. Permitted Uses and Disclosures of De-Identified Information. A covered entity may create information that is not individually identifiable health information by using protected health information to create de-identified health information. The information is no longer protected health information after it is de-identified. It may use de-identified information or disclose the protected health information to be de-identified only to business associates for the purpose of de-identification, whether or not the information is to be used by the covered entity. In order to be eligible for the uses and disclosures, the information needs to meet the standard for the de-identification in 45 C.F.R. § 164.514(a) and (b), and any codes used with respect to the de-identified information may not be disclosed.¹¹²
- D. Permitted Disclosure or Use of a Limited Data Set. A limited data set may be disclosed only for the purposes of research, public health or health care operations.¹¹³ A limited data set may use protected health information to create the limited data set to disclose the limited data set only for the purposes of research, public health or health care operations, such as providing the limited data set to review quality of care.¹¹⁴ A limited data set may be disclosed as long as there is a data use agreement that satisfies the standards in the regulation and that specifies the recipient will only use or disclose protected health information for the limited use purposes.

¹⁰⁹ OCR Guidance Explaining Significant Aspects of the Privacy Rule, Uses and Disclosures for Treatment, Payment and Health Care Operations, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

¹¹⁰ *Id.*

¹¹¹ 45 C.F.R. § 164.502 (2000).

¹¹² 45 C.F.R. § 164.502(d) (2000).

¹¹³ 45 C.F.R. § 164.514(e)(3)(i) (2002).

¹¹⁴ 45 C.F.R. § 164.514(e)(3)(ii) (2002).

1. Limited Data Set Defined. A Limited Data Set is protected health information that excludes the following identifiers of the individual, or of relatives, employers or household members of the individual:
 - a. Names;
 - b. Postal address information, other than town or city, state and zip code;
 - c. Telephone numbers;
 - d. Fax numbers;
 - e. Electronic mail addresses;
 - f. Social Security numbers;
 - g. Medical record numbers;
 - h. Health plan beneficiary numbers;
 - i. Account numbers;
 - j. Certificate/license numbers;
 - k. Vehicle identifiers and serial numbers, including license plate numbers;
 - l. Device identifiers and serial numbers;
 - m. Web Universal Resource Locators (URLs);
 - n. Internet Protocol (IP) address numbers;
 - o. Biometric identifiers, including finger and voice prints; and
 - p. Full face photographic images and any comparable images.¹¹⁵

2. Limited Data Set Agreement Standards. A limited data set use agreement must satisfy all of the following requirements and be executed between a

¹¹⁵ 45 C.F.R. § 164.514(e)(2) (2002).

covered entity and the limited data set recipient. The data use agreement must:

- a. Establish the uses and disclosures of the limited data set by the recipient in compliance with the purposes described above in B., and it must not permit the recipient to use or disclose the information in any way that would not be permitted if done by the covered entity;
- b. Establish who is permitted to use or receive the limited data set; and
- c. Require that the recipient will:
 - (i) not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
 - (ii) use appropriate safeguards to prevent use or disclosure of the information in any manner not provided for by the agreement;
 - (iii) report to the covered entity any use or disclosure of the information that is not provided for in the agreement of which the recipient becomes aware;
 - (iv) ensure that any agents or subcontractors to whom it provides the data agrees to the same restrictions and conditions that apply to the recipient under the agreement; and
 - (v) not identify the information or contact the individuals.¹¹⁶

3. Consequence of Pattern of Violations. If a covered entity knows of a pattern of activity or a practice of a limited data set recipient that constitutes a material breach or violation of the data use agreement, the covered entity is not in compliance with the standard unless it took reasonable steps to cure the breach or end the violation. If such steps were unsuccessful, the covered entity must discontinue disclosure to the recipient and report the problem to the Secretary of HHS.¹¹⁷ If a covered entity is a limited data set recipient and it violates its data use agreement, it will be in violation of the standard for the limited data set and may be subject to civil or other penalties.¹¹⁸

- E. Permitted Disclosure to Business Associates. A covered entity may disclose protected health information to a business associate and allow the business associate

¹¹⁶ 45 C.F.R. § 164.514(e)(4) (2002).

¹¹⁷ 45 C.F.R. § 164.514(e)(5)(A) (2002).

¹¹⁸ 45 C.F.R. § 164.514(e)(5)(B) (2002).

to create or receive protected health information on its behalf if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. However, this requirement does not apply to any covered entity for (1) disclosure by a covered entity to a health care provider concerning treatment of the individual, (2) with respect to disclosures by a group health plan or health insurance issuer or HMO with respect to the group health plan to the plan's sponsor for obtaining preliminary bids, modifying, amending or terminating the plan or to provide information on enrollment, disenrollment or whether an individual is participating, (3) if the disclosure is by a group health plan that is a governmental program providing public benefits, or if the protected information is used to determine enrollment or eligibility in the health plan if collected by an agency other than the agency administering the health plan and that is authorized by law.

If a covered entity violates the satisfactory assurance requirement it made as a business associate of another covered entity, the covered entity violating the satisfactory assurance request is in non-compliance with the privacy standards.¹¹⁹ The covered entity must document the satisfactory assurances to safeguard the information it received from business associates either in a written contract or written agreement or an arrangement with the business associate.¹²⁰ A business associate contract is not required with persons or entities whose functions, activities or services do not involve the use or disclosure of protected health information, and where any access by such persons would be incidental, if at all, e.g., janitorial services. However, if the entity performs services for a covered entity where the access to protected health information is not limited in nature, such as shredding documents or routinely handling records containing protected health information, it would be a business associate. However, if such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), then the covered entity may treat the service provider as part of its work force and no business associate agreement is necessary.¹²¹

In guidance issued by the Office for Civil Rights, it is stated that a stop loss insurer is generally not a business associate of a health plan solely by selling a stop loss policy to a health plan and paying claims under the stop loss policy. It also indicates that a business associate relationship could arise if the stop loss insurer performs a function on behalf of or provides services to the health plan.¹²² However, many stop loss policies are sold to the employer in the single employer plan arena, and the guidance does not address that factual situation.

¹¹⁹ 45 C.F.R. § 164.502(e) (2000).

¹²⁰ 45 C.F.R. § 164.502(e) (2000).

¹²¹ OCR Guidance Explaining Significant Aspects of Privacy Rule, Business Associates, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

¹²² OCR Guidance Explaining Significant Aspects of Privacy Rule, Business Associates, found at www.hhs.gov/ocr/hipaa/privacy.html.

The guidance further explains that a software vendor who sells or provides software to a covered entity, but does not have access to protected health information is not a business associate. However, if the software vendor needs access to the protected health information to provide its services, then the vendor is a business associate, e.g., if the software vendor installs and tests the software on an information system and will be given access to the protected health information on such system as part of its testing. However, if an employee of a contractor, such as a software vendor, has his primary duty station on-site at the covered entity, the covered entity may choose to treat such employee as a member of the covered entity's work force.¹²³

1. Business Associate Agreement Standards. Disclosures to a business associate require that there be a written agreement. The business associate contracts must also meet certain standards. A business associate contract is a contract between a covered entity and its business associate. A covered entity will not be treated as in compliance if it knows of a pattern or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under the contract or any other arrangement, unless the covered entity takes reasonable steps to cure the breach or end the violation. If any such steps to cure a breach were unsuccessful, the covered entity must terminate the contract, if feasible, or if it cannot terminate the contract, then it must report the problem to the Secretary of HHS.

Business associate contracts must establish the permitted and required uses and disclosures of information by the business associate and may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the privacy regulations, if the use or disclosure was done by the covered entity. However, a business associate contract may permit the business associate to use or disclose protected health information for the proper management and administration of a business associate and it may permit the business associate to provide data aggregation services relating to health care operations of the covered entity.

The business associate contract must provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or required by law; that the business associate will use safeguards to prevent use or disclosure of the information in any manner other than as provided for in the contract; the business associate will report to the covered entity any use or disclosure of the information that is not provided for by the contract when it becomes aware of such use or disclosure; that the contract will ensure that any agents, including any subcontractors to

¹²³ *Id.*

whom the business associate provides protected health information, received from or created by business associate on behalf of the covered entity, will agree to the same restrictions and conditions that apply to the business associate regarding the protected health information. The business associate contract must also provide for making available protected health information to individuals who are the subject of the protected health information and must make available protected health information for amendment and incorporation of any amendments into the protected health information based on an individual's request to amend such information. The business associate contract must require the business associate to provide an accounting of any disclosure of protected health information to the individual who is the subject of the protected health information. The business associate contract must make the business associate's internal practices, books and records relating to the use and disclosure of protected health information received from or created by the business associate on behalf of the covered entity available to the Secretary of HHS for the determination of compliance. At the termination of the contract, the business associate must return or destroy all protected health information received from, or created or received by, the business associate on behalf of the covered entity. Thus if the business associate still maintains the protected information in any form, it either must retain no copies of such information, or if the return or destruction is not feasible, it must extend the protection of the contract for the information and limit future use and disclosure for the duration of the period that makes the return and destruction of the information infeasible.¹²⁴

The business associate contract must authorize the termination of the contract by the covered entity if the covered entity determines that the business associate had violated a material term of the contract. There are special rules for situations in which the business associate and the covered entity are both governmental entities.¹²⁵ The agreement between the business associate and the covered entity may permit the associate to use the information it receives in its capacity as a business associate to the covered entity, if necessary, for proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.¹²⁶ The business associate may disclose the protected information if this disclosure is required by law, or the business associate obtains reasonable assurance from the person to whom the information is disclosed that it will be held confidentially and used or disclosed only as required by law for the purpose for which it was disclosed and the person notifies the business associate of any instance of which it is aware in which the confidentiality of the information has been

¹²⁴ 45 C.F.R. § 164.504(e) (2000).

¹²⁵ 45 C.F.R. § 164.504(e) (2000).

¹²⁶ 45 C.F.R. § 164.504(e)(4) (2000).

breached.¹²⁷ A model business associate agreement was included in the appendix to the preamble to the final modifications which differed from the model agreement previously issued.¹²⁸ Additional requirements are imposed on the business associate agreement by the Final Security Regulations issued on February 20, 2003, at 45 C.F.R. Parts 160, 162 and 164.

- F. Permitted Disclosure Regarding Deceased Individuals. The privacy regulations apply with respect to deceased individuals and the covered entities must treat a decedent's personal representative as the individual for purposes of the privacy requirements.¹²⁹ The covered entity may disclose protected health information to a coroner or medical examiner for purposes of identifying a deceased person, determining the cause of death, or other duties authorized by law. A covered entity may also disclose protected health information to funeral directors, as necessary to carry out their duties with respect to the decedent. This information may also be disclosed to funeral directors prior to or in anticipation of the individual's death if it is necessary for the funeral directors to carry out their duties.¹³⁰
- G. Permitted Disclosures to Personal Representatives. The covered entity must treat a person as the personal representative of an individual unless the covered entity has a reasonable belief that the individual has been or may be subject to domestic violence, abuse and neglect by such person, or the treating of such person as the personal representative could endanger the individual and the covered entity decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.¹³¹ Special rules apply for unemancipated minors.¹³² A power of attorney must specifically include decisions related to health care in order for it to authorize the holder to exercise the individual's rights under the HIPAA privacy rule.¹³³ If under local law, a parent, guardian or individual or individual who is acting *in loco parentis* who has the authority to act on behalf of an unemancipated minor with respect to health considerations, the covered entity must treat such person as a personal representative except when the minor consents to the health care and no other consent is required by law and the minor has not asked the person to be his personal representative.

¹²⁷ 45 C.F.R. § 164.504(e)(4)(ii) (2000).

¹²⁸ 67 F.R. 53181, 53264 (2002).

¹²⁹ 45 C.F.R. § 164.502(f) (2000).

¹³⁰ 45 C.F.R. § 164.512(g) (2000).

¹³¹ 45 C.F.R. § 164.502(g) (2000).

¹³² 45 C.F.R. § 164.502(g) (2000).

¹³³ OCR Guidance Explaining Significant Aspects of Privacy Rule, Personal Representatives, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

If a covered entity is required or permitted by state law to provide access to the health information of an unemancipated minor to a parent, guardian or person acting *in loco parentis*, the covered entity may disclose the protected health information to such person. If a covered entity is prohibited by state law from disclosing information about an unemancipated minor to a parent, guardian or person acting *in loco parentis*, the covered entity must not disclose such information.

Where a parent or other person *in loco parentis* is not the personal representative of the unemancipated minor and applicable state law does not provide access, a covered entity may provide or deny access to protected health information about a minor to a parent, guardian or other person activity *in loco parentis* provided the decision about the access or denial is made by the licensed health care provider in the exercise of its professional judgment.¹³⁴

H. Other Permitted Disclosures.

1. Disclosure by Work Force/Business Associate on Good Faith Belief of Violation. The covered entity will not be considered to have violated the privacy requirements if a member of its work force or its business associate directly discloses the protected health information, provided that the work force member or business associate, believes in good faith, that the covered entity engaged in conduct that is unlawful or otherwise violates professional and clinical standards or the care, services or conditions provided by the covered entity potentially endangers one or more patients, workers or the public, and the disclosure is made to a health oversight agency or public health authority, or to an attorney retained by or on behalf of the work force member or business associate for the purposes of determining the legal options of the member or business associate.¹³⁵ The Sarbanes-Oxley Act of 2002 enacted additional protections for whistleblowers by adding to 18 USC § 1513 new paragraph (e) which provides that whoever knowingly takes any action harmful to any person, including interference with the lawful employment or likelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than ten years or both.¹³⁶ The Sarbanes-Oxley Act also increased the penalties under section 501 of the Employee Retirement Income Security Act of 1974, as amended (“ERISA”) for a willful violation by an individual to a fine of not more than \$100,000 (previously \$5,000), to up to ten years imprisonment (previously one) and for a willful violation by an

¹³⁴ 45 C.F.R. § 164.502(g)(3)(ii) (2002).

¹³⁵ 45 C.F.R. § 164.502(j) (2000).

¹³⁶ P.L. 107-210, § 1107 (2002).

entity, to a fine of up to \$500,000 (previously \$100,000).¹³⁷ The provisions in Part 1 of ERISA include section 402's requirement that the plan be established and maintained pursuant to a plan document, which under the privacy regulations must include the plan's provisions on compliance with privacy. Thus, violation of a plan's privacy provisions may have additional consequences beyond enforcement by the Department of Health and Human Services.

2. Disclosures to Law Enforcement Regarding Suspected Perpetrators of Criminal Acts. If a member of the work force of a covered entity, who is the victim of a criminal act, discloses protected health information to a law enforcement official, the covered entity is not considered to have violated the requirements of the privacy regulations if the protected information disclosed is about the suspected perpetrator of the criminal act and the information disclosed is limited to information and the standards for disclosure to law enforcement officers for the use in identifying or locating a suspect, fugitive or material witness or missing person, and provided no more than the name, address, date and place of birth, social security number, ABO blood type and Rh factor, the type of injury, the date and time of the treatment, date and time of death, or the description of any distinguishing characteristics.¹³⁸ For example, if a doctor was stabbed by a mentally ill patient in the emergency room, the doctor could tell the police the above information regarding the patient who stabbed her without violating the privacy regulations.

I. Permitted Uses and Disclosures by a Group Health Plan. The privacy regulations also provide that a group health plan may engage in certain uses and disclosures. A group health plan may disclose protected health information to a plan sponsor to carry out the plan administration functions (as defined above) with respect to the plan (e.g., adjudicating claims, obtaining renewals) that the plan sponsor provides. A group health plan may not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor unless the notice to the employees regarding the uses and disclosure of individual health information includes in the notice this use or disclosure as one of the uses or disclosures. A group health plan may not disclose protected health information to the plan sponsor for purposes of employment related actions or decisions or in connection with any other benefit or employee benefit plan.¹³⁹ (For example, the employer who notes its forklift operator is obtaining excessive narcotics prescriptions is not supposed to stop the individual from operating heavy equipment or fire him.) A group health plan may disclose summary health information to the plan sponsor if the plan sponsor requests it for purposes of obtaining bids for insurance or for modifying, amending or

¹³⁷ P.L. 107-210, § 904 (2002).

¹³⁸ 45 C.F.R. § 164.502(j)(2) and § 164.510(f) (2000).

¹³⁹ 45 C.F.R. § 164.504(f)(3) (2000).

terminating the plan.¹⁴⁰ A group health plan may disclose to the plan sponsor information on whether an individual is participating, enrolled or disenrolled.¹⁴¹

1. Special Requirements for Group Health Plans. In order for a group health plan to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by health insurance issuer or HMO, the group health plan must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of the privacy regulations. This will affect the contents of the plan document which will need to include the restrictions on uses and disclosures of information adopted by the plan sponsor in compliance with the privacy regulations.¹⁴² The Final Security Regulations issued on February 20, 2003, also impose additional requirements on the contents of the group health plan's document.¹⁴³

2. Plan Document Requirements. The plan documents of the group health plan must be amended to incorporate provisions to do the following: (1) establish the permitted and required uses and disclosures of the information by the plan sponsor provided that such permitted and required uses and disclosures may not be inconsistent with the privacy regulations,¹⁴⁴ (2) must provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to the following: (a) it will not use the disclosed information other than as permitted or required by the plan documents or as required by law (a plan sponsor may be required by law to report an OSHA violation that it first learns of from the group health plan if the group health plan discloses information that constitutes a reportable event under OSHA (*See* 29 C.F.R. § 1904.29(b)(3) and 29 C.F.R. § 1904.44(b)(i) and 29 U.S.C.S. § 654(a)(1) and 657); the definition of "required by law" at 45 C.F.R. § 164.501 (2000) was modified by the final modifications so that required by law is a requirement on an entity and not a covered entity. Thus a requirement on the employer now meets the regulation's definition of "required by law" and an employer who receives information of a potential OSHA issue from the group health plan may disclose or use that information

¹⁴⁰ 45 C.F.R. § 164.504(f)(2002).

¹⁴¹ 45 C.F.R. § 164.504 (f)(1)(iii)(2002).

¹⁴² 45 C.F.R. § 164.504(f)(1) (2000).

¹⁴³ 45 C.F.R. § 164.314(b) (2003).

¹⁴⁴ 45 C.F.R. § 164.504(f)(2)(i) (2000).

as necessary to comply with the requirements imposed by OSHA)¹⁴⁵; (b) it ensures that any agents, including subcontractors, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information; (c) it will not use or disclose the information for employment related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor; (d) it will report to the group health plan any use or disclosure of the information that is inconsistent with the use or disclosure for which it was provided and of which it becomes aware; (e) to make available protected health information in accordance with an individual's request to access to their individual health information; (f) it will make available protected health information for amendment and to incorporate any amendments into protected health information in accordance with the procedures under the privacy regulations for an individual who requests amendment of his/her individual health information; (g) it will make available information required to provide an accounting of any disclosures as required by the privacy regulations; (h) it will make its internal policies or practices, books and records relating to use and disclosure of protected health information received from a group health plan available to the Secretary of HHS in order to determine the compliance of the group health plan with the privacy regulations; (i) if feasible, it will return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which the disclosure was made, except that, if such return or destruction is not feasible, it agrees to limit future uses and disclosures to those purposes that make the return or destruction of the information infeasible; and (j) it will ensure that the adequate separation required by 45 C.F.R. § 164.504(f)(2)(iii) of the privacy regulations with respect to separation between the group health plan and the group health sponsor is established.¹⁴⁶

3. Separation between Group Health Plan and Plan Sponsor. In order for there to be adequate separation between the group health and the plan sponsor, the plan documents must further provide: (1) a description of those employees or classes of employees or other persons under the control of the plan sponsor to be given access to protected health information to be disclosed, provided that any employee or person who receives protected health information relating to

¹⁴⁵ Required by law is defined in 45 C.F.R. § 164.501 (2000) as a mandate that compels a covered entity that is enforceable in a court of law to make a use for disclosure of protected health information. The definition originally assumed disclosures only by a covered entity and the plan sponsor in many cases will not be a covered entity. However, the definition of required by law was changed by the final modifications issued on August 14, 2002, to be defined as a mandate that compels an entity that is enforceable in a court of law; thus, permitting entities who have received protected health information to disclose the information even though they are not covered entities. 45 C.F.R. § 164.501 (2002).

¹⁴⁶ 45 C.F.R. § 164.504(f)(2) (2000).

payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description (these persons also must be trained on HIPAA's requirements); (2) restrictions on the access to and use by such employees and other persons to plan administration functions that the plan sponsor performs for the group health plan; and (3) to provide an effective mechanism for resolving any issues of noncompliance by the persons who are authorized above to receive information that the plan document provisions required by the regulations.¹⁴⁷

For purposes of this section, plan administration functions are defined as functions performed by the plan sponsor on behalf of the group health plan and excludes functions performed by the plan sponsor, or decisions with respect to, or in connection with any other benefit or benefit plan of the sponsor.¹⁴⁸

- J. Permitted Use or Disclosure for Treatment, Payment or Health Care Operations by a Health Care Provider. The final regulation substantially rewrote the requirements related to use of protected health information for treatment, payment and health care operations. For any use or disclosure to be used to carry out treatment, payment or health care operations, the health care provider may use or disclose protected health information to carry out treatment, payment or health care operations as long as an authorization is not required for either the use of psychotherapy notes, or to use the information for marketing. A health care provider may obtain consent of an individual to use or disclose protected health information for treatment, payment or health care operations, but such consent will not permit a use or disclosure that is not otherwise permitted by the regulations, nor will it permit disclosure or use when another condition must be met for the disclosure to be permissible under the privacy regulations.¹⁴⁹ A covered entity may disclose protected health information to a health care provider for treatment activities of a health care provider.¹⁵⁰ A covered entity may disclose protected health information to another covered entity or health care provider for payment activities of the entity that receives the information, this would include a health care provider's disclosure to a health plan for payment.¹⁵¹ A covered entity may disclose protected health information to another covered entity for certain health care operations of the recipient entity if each of the entities has or had a relationship with the individual who is the subject of the information, the protected health information pertains to the relationship, and the disclosure is either:

¹⁴⁷ 45 C.F.R. § 164.504(f)(2)(iii) (2000).

¹⁴⁸ 45 C.F.R. § 164.504(a) (2000).

¹⁴⁹ 45 C.F.R. § 164.506 (a) and (b) (2002).

¹⁵⁰ 45 C.F.R. § 164.506(c)(2) (2002).

¹⁵¹ 45 C.F.R. § 164.506 (2000); 45 C.F.R. § 164.506(c)(3) (2002).

1. for conducting quality assessment and improvement activities (as defined in 45 C.F.R. § 164.501 health care operations definition (1)) including outcome evaluation and development of clinical guidelines provided that obtaining generalized knowledge is not the primary purpose of any studies resulting from such activities;
2. for reviewing the competence or qualification of health care professionals, evaluating practitioner and provider performance, health plan performance (as defined in 45 C.F.R. § 164.501 health care operations definition (2)); or
3. for purposes of health care fraud and abuse detection.¹⁵²

A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.¹⁵³

The final modifications deleted the regulations that provided that the health care provider may condition treatment on the provision by the individual of the consent for release of information for payment, treatment or health care operations and that the health plan may condition enrollment on the provision by the individual of consent, if consent is sought in conjunction with enrollment.

III. Uses or Disclosures for Which Authorization is Required. There are a number of uses other than disclosures for which authorization is required. Any use or disclosure must be consistent with the authorization for the particular use or disclosure.¹⁵⁴

A. Use or Disclosure of Psychotherapy Notes. A covered entity must obtain authorization for any use or disclosure of psychotherapy notes. Psychotherapy notes are notes recorded by health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session that is separated from the rest of the individual's medical records. Psychotherapy notes do not include medication and prescription monitoring, counseling sessions start and stop times, the modalities and frequencies of treatment furnished, results of clinical test and any summary of the following items, diagnosis, functional status, treatment plan, symptoms, and prognosis of progress to date.¹⁵⁵ Authorization is not required for disclosure of psychotherapy notes for treatment, payment or health care operations, for use by the originator for treatment, for use or disclosure by a covered entity in training programs

¹⁵² 45 C.F.R. § 164.506(c) (2002).

¹⁵³ 45 C.F.R. § 164.506 (c)(5) (2002).

¹⁵⁴ 45 C.F.R. § 164.508(a) (2000).

¹⁵⁵ 45 C.F.R. § 164.501 (2000).

in which students learn to supervise, practice or improve their skills in group, joint, family or individual counseling, for use to defend itself in a legal action, to defend itself in a proceeding or other action brought by the individual, for any use or disclosure that is required to comply with the Secretary of HHS's requirements to determine compliance with the privacy regulations or that are permitted as disclosures required by law that are limited to the relevant requirements of the law, for disclosures for health care oversight activities of the originator of the psychotherapy notes, for disclosures to coroner or medical examiner to use to identify the deceased or determine the cause of death, or if the covered entity determines that the use or disclosure is necessary to lessen or prevent serious or imminent threat to the health and safety of a person or the public and the disclosure is made to a person who is reasonably able to prevent or lessen the threat, or the disclosure is necessary to apprehend an individual he/she believes committed a crime because of a statement admitting participation in a violent crime that the covered person believes may have caused serious physical harm to the victim, or the covered person believes the individual to be a person who escaped from lawful custody.¹⁵⁶

B. Authorization for Marketing. A covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except for marketing communications in the form of:

1. face-to-face communication made by a covered entity to an individual; or
2. a promotional gift of nominal value provided by the covered entity (e.g., sample shampoo);

If the marketing involves direct remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.¹⁵⁷

Marketing under the final regulations includes a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about the entities participating in the provider network, replacement of or enhancements to a health plan, and health related products or services only available to a health plan enrollee that add value to, but are not part of a plan of benefits.¹⁵⁸

¹⁵⁶ 45 C.F.R. § 164.508(a) (2000); 45 C.F.R. § 164.508(a)(2) (2002).

¹⁵⁷ 45 C.F.R. § 164.508(a)(3) (2002).

¹⁵⁸ 45 C.F.R. § 164.501 (2002).

Thus, the focus of the marketing definition changed from the purpose of the communication to the effect of the communication. The modifications substantially shortened the definition of what constitutes marketing.

The new marketing definition excludes communications to an individual to describe the entities participating in the provider network or health plan network or to describe if and to the extent a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits. The new definition also excludes communications to an individual for treatment of the individual or for case management or care coordination for the individual, or for alternate treatments, therapies, health care providers or settings of care for that individual.¹⁵⁹ The guidance issued by the OCR indicates that a health plan sending information to subscribers approaching Medicare eligibility regarding Medicare supplement policies is not marketing.¹⁶⁰ Query: Is a pharmacy benefit manager who sends prescription refill reminders doing it in the interest of the covered entity or in its own interest thus making it marketing?

- C. Combination of Authorization for Disclosure or Use with Notice. There are restrictions on combining the notice with the authorization or with other documents particularly with respect to psychotherapy notes.¹⁶¹ An authorization can only be combined in certain manners and there is a prohibition on conditioning treatment, payment, enrollment and health plan eligibility for benefits on the provision of the authorization except in the following circumstances: (a) if it is research related treatment, or (b) the health plan may condition enrollment and health plan or eligibility for benefits on the provision of the authorization requested by the health plan prior to the individual's enrollment in the health plan if the authorization is sought for the health plan's eligibility or enrollment determinations relating to the individual for its underwriting or risk rating determinations, and (c) the authorization is not for use or disclosure of psychotherapy notes. A health plan may condition payment of claim for specified benefits on provisions of the authorization, if the disclosure is necessary to determine payment of the claim and the authorization is not for use or disclosure of psychotherapy notes. The covered entity may condition the provision of health care on an authorization created solely for the purposes of creating protected health information for disclosure of such intent to such third party.¹⁶²

¹⁵⁹ 45 C.F.R. § 164.501(2002).

¹⁶⁰ OCR Guidance Explaining Significant Aspects of Privacy Rule, Marketing, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

¹⁶¹ 45 C.F.R. § 164.508(b)(3) (2000) and 45 C.F.R. § 164.508(b)(3) (2002).

¹⁶² 45 C.F.R. § 164.508(b) (2002).

D. Standards for a Valid Authorization. Any authorization for disclosure must be valid and have an expiration date.¹⁶³ Any authorization must contain certain elements including, a statement the covered entity will not condition treatment, payment, enrollment in the health plan or eligibility for benefits on the individual's providing authorization; a description of each purpose for a requested use or disclosure, a statement that the individual can inspect and copy the protected health information to be used or disclosed; that the individual may refuse to sign the authorization, and if the use or disclosure will result in a direct or indirect remuneration of the covered entity from a third party, a statement that the remuneration will result must be made. The individuals must be provided with a copy of the signed authorization.¹⁶⁴ Special rules apply to authorizations related to research.¹⁶⁵

1. A health plan may condition enrollment or eligibility for benefits on an individual's providing an authorization prior to enrollment if the authorization is sought for the health plans eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations and the authorizations is not for a use or disclosure of psychotherapy notes.¹⁶⁶ An individual may revoke an authorization, provided, the covered entity has not taken action relying upon the authorization or it was not provided as a condition for obtaining insurance coverage and another law or the policy provides the insurer with the right to contest the claim.¹⁶⁷
2. An authorization must include certain items in addition to the core elements.¹⁶⁸ The other elements that must be included are statements putting the individual on notice of:
 - a. the individual's right to revoke the authorization in writing and either;
 - i.. the exceptions to the right to revoke and a description of how to revoke the authorization; or
 - ii. the extent of the right to revoke and a statement that an explanation of how to revoke is included in the privacy notice (a reference to the covered entity's notice).

¹⁶³ 45 C.F.R. § 164.508(c) (2002).

¹⁶⁴ 45 C.F.R. § 164.508(a), (b), (c) and (d) (2002).

¹⁶⁵ See 45 C.F.R. § 164.508(b)(3)(i) and (b)(4) (2002).

¹⁶⁶ 45 C.F.R. § 164.508(b)(5) (2002).

¹⁶⁷ 45 C.F.R. § 164.508(b)(5) (2002).

¹⁶⁸ 45 C.F.R. § 164.508(c) (2002).

- b. the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization by either:
 - i. stating the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs an authorization for benefits; or
 - ii. the consequences to the individual of refusing to sign the authorization when an entity can condition treatment, enrollment in the health plan or eligibility for benefits on obtaining the authorization.
 - c. the potential for information disclosed pursuant to an authorization to be redisclosed by the recipient and no longer to be protected by the privacy regulations.¹⁶⁹
- 3. Special requirements apply to authorizations for research.¹⁷⁰
 - 4. If a covered entity seeks an authorization from an individual, it must provide the individual with a copy of the signed authorization.¹⁷¹

IV. Use or Disclosure with Opportunity to Agree or Object. There are a number of uses or disclosures that require an opportunity for an individual to agree or object. In this case, the covered entity may use or disclose the information without written authorization of the individual, provided the individual is informed in advance of the use or disclosure and has the opportunity to agree, prohibit or restrict a disclosure as provided in the regulations. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure that is covered in this IV.

A. Facility Directories. An individual has an opportunity to agree or object to the use or disclosure of his name and general condition in a facility directory. The covered health care provider may use the following information to manage or direct individuals of that facility: the individual's name, the individual's location in the covered health care providers facility, the individual's condition described in general terms that does not communicate any specific medical information, and the individual's religious affiliation may be disclosed for directory purposes to members of the clergy or to other persons who ask for the individual by name, as long as the religious affiliation is not disclosed to individuals who are not clergy.¹⁷² The individual must be informed of the opportunity to object to inclusion of his

¹⁶⁹ 45 C.F.R. § 164.508(c)(2) (2002).

¹⁷⁰ 45 C.F.R. § 164.508(c) (2002).

¹⁷¹ 45 C.F.R. § 164.508(c)(4) (2002).

¹⁷² 45 C.F.R. § 164.510(a)(1) (2000).

information in the directory and be informed of the persons to whom the health care entity may disclose the information. The individual must be provided with the opportunity to restrict or prohibit some or all of the uses or disclosures. In the case of an emergency where the opportunity to object to uses or disclosures cannot practicably be provided because of the individual's incapacity or emergency treatment circumstances, a health care provider may use or disclose some or all of the protected health information described above for the facilities directory, if the disclosure is consistent with prior expressed preferences of the individual, if any, and if it is in the individual's best interest as determined by the covered health care provider, provided, the health care provider informs the individual and provides the opportunity to object to the use or disclosures for directory purposes when it is practicable to do so.¹⁷³

- B. Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes. A covered entity may disclose to family members, other relatives, a close personal friend of the individual, or any person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's care, or payment related to the individual's health care. The covered entity may use or disclose protected health information to notify or assist in notification of, including identifying or locating a family member, a personal representative of the individual, or another person responsible for the care of the individual's location, general condition or death.¹⁷⁴
- C. Uses and Disclosures When the Individual is Present. If the individual is present and has the capacity to make health care decisions, the covered entity may use or disclose protected health information if it obtains the individual's agreement, provides the individual with the opportunity to object to a disclosure and the individual does not express an objection, or if the health care provider reasonably infers from the circumstances that the individual does not object to disclosure.¹⁷⁵
- D. Use and Disclosure When the Individual is Not Present. If the individual is not present, and the opportunity to agree or object to a use or disclosure and cannot be provided the opportunity to agree or object, or the opportunity cannot practicably be provided because of the individual's incapacity or emergency circumstances, the covered entity may determine whether disclosure is in the best interest of the individual and if so, disclose only the protected health information directly relevant to the person and for limited follow-up with the individual's health care.¹⁷⁶
- E. Use and Disclosures for Disaster Relief. The covered entity may use and disclose protected health information for disaster relief purposes to a public or private entity

¹⁷³ 45 C.F.R. § 164.510(a) (2000).

¹⁷⁴ 45 C.F.R. § 164.510(b) (2000).

¹⁷⁵ 45 C.F.R. § 164.510(b)(2) (2000).

¹⁷⁶ 45 C.F.R. § 164.510(b)(3) (2000).

authorized by law or by its charter to assist with disaster relief efforts for purposes of coordinating such entities.¹⁷⁷

V. Uses and Disclosures for Which No Authorization or Opportunity to Agree or Object is Required. There are also uses and disclosures for which an authorization or an opportunity to agree or object is not required. In these situations, the covered entity may use or disclose protected health information without obtaining written authorization of the individual and without providing the individual with an opportunity to agree or object. If the covered entity is required to inform the individual of the disclosure or use of information, the covered entity may inform the individual orally and may obtain the individual's agreement orally.¹⁷⁸ The 2002 modifications to the final rule deleted the reference to no need for consent for these types of disclosures.

A. Uses and Disclosures "Required by Law". To the extent use or disclosure is required by law, the use or disclosure complies with and is limited to the relevant requirements of the law, the covered entity may disclose protected health information.¹⁷⁹ A disclosure is required by law if there is a mandate that compels an entity to make a use or disclosure of protected health information which is enforceable in court.¹⁸⁰ Required by law includes statutes or regulations that require production of information.¹⁸¹ However, the reporting requirements under OSHA apply to an employer; thus, the change in the final modifications to the "required by law" definition changed the requirement and permitted disclosure by the entity (and not just a covered entity) to permit an employer who receives the protected health information from the plan that might indicate a potential OSHA reportable event for the employer to disclose or use that information because the employer is an entity and meets the new requirements under the privacy regulation.¹⁸² A disclosure to the Maine Health Data Organization ("MHDO") pursuant to Maine statute was a disclosure "required by law" and permitted by the third party administrator's agreements with the ERISA plans, and nothing in the state law conflicts with ERISA, thus the court granted summary judgment for defendant on the plaintiff's complaint alleging the Maine statute was preempted.¹⁸³

B. Disclosures for Public Health Activities. A covered entity may disclose protected health information for public health activities to:

¹⁷⁷ 45 C.F.R. § 164.510 (2000).

¹⁷⁸ 45 C.F.R. § 164.512 (2000).

¹⁷⁹ 45 C.F.R. § 164.512(a) (2000).

¹⁸⁰ 45 C.F.R. § 164.103 (2003).

¹⁸¹ 45 C.F.R. § 164.103 (2003).

¹⁸² 45 C.F.R. § 164.103 (2003) and 29 C.F.R. §§ 1904.29(b)(3) and 1904.44(b)(i).

¹⁸³ *Patient Advocates, LLC v. Prysunka*, 2004 U.S. Dist. LEXIS 682 (D.C. Maine 2004).

1. a public health authority that is authorized by law to collect and receive such information for purposes of preventing or controlling disease, injury, disability, including reporting disease, injury, vital elements such as births and deaths and the conduct of public health surveillance, public health investigations and public health interventions or at the direction of the public health authority to an official of the foreign government who is acting in collaboration with the public health authority;
2. the public health authority or public government authority authorized by law to receive reports of child abuse and neglect;
3. a person subject to the jurisdiction of the Food and Drug Administration with respect to an FDA regulated product or activity for which such person has responsibility for purposes related to quality, safety or efficacy of the product or activity, including: (a) reporting adverse events, prior defects or problems or biological product deviations, (b) to track FDA regulated products, (c) to enable product recalls, repairs and replacements, or (d) to conduct post marketing surveillance;¹⁸⁴
4. a person who may have been exposed to communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person, as necessary, in the conduct of public health intervention or investigation; or
5. by a health care provider to an employer about an individual who is a member of the work force for the employer, if the covered entity is a covered health care provider who is a member of a work force of such employer, or if the health care provider provides health care to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the work place or to evaluate whether the individual has a work related illness or injury. This appears to address disclosures by a health care provider to an employer for OSHA compliance, drug screening and worker's compensation; however, the extent of this disclosure is still to be clearly defined. The ability to disclose is only given to health care providers, not health plans. The protected health information that is disclosed must consist of findings considering work related illness or injury or work place related medical surveillance. The employer must need such information in order to comply with its obligations under 29 C.F.R. § 1904-1928 (the Occupational Safety and Health Act (“OSHA”)), 30 C.F.R. § 50-90 (The Federal Mine Safety and Health Act) or under state law with the similar purpose to record such illness or injury to carry out responsibilities for work place medical surveillance.

¹⁸⁴ 45 C.F.R. § 164.512 (2002).

The health care provider must provide written notice to the individual that protected health information relating to medical surveillance in the work place of work related illness and injury are disclosed to the employer by giving a notice to the individual at the time the health care is provided, or if health care is provided on the work site of the employer, by posting notice in a prominent place at the location where the health care is provided.¹⁸⁵ Disclosures to an employer of pre-employment physicals, drug tests or fitness for duty without the authorization of the individual are permitted only in limited circumstances. If there is no authorization for disclosure by the individual, the covered entity may only disclose the protected health information to the individual's employer if the covered entity provided health care to the individual at the request of the employer or as a member of the employer's work force, the medical services must relate to the medical surveillance of the workplace or evaluation of whether the individual has a work-related illness or injury, and the employer has a duty under the Occupational Safety and Health Administration or the Mine Safety and Health Administration or a similar State law to keep records on or to act on such information. Since employment physicals, drug tests and fitness for duty exams are often not provided with all of the requirements above, employers will need to obtain the individual's authorization to be able to access such protected health information from the health care provider. While such information is protected health information in the hands of the health care provider, if the employer receives it in its capacity as employer, it becomes employment medical records, provided it is not paid for by the employer's health plan.¹⁸⁶ Employee medical records are frequently subject to state law requirements on confidentiality.

Note the above are only for disclosures for public health activity. Uses for public health activities in 1, 2, 3 and 4 above are only available to a covered entity that is also a public health authority.¹⁸⁷

- C. Disclosures Regarding Victims of Abuse, Neglect or Domestic Violence. A covered entity may disclose protected health information about an individual the covered entity reasonably believes to be a victim of abuse, neglect or domestic violence to government authority, including a social service or protective services agency, that is authorized by law to receive reports of abuse, neglect and domestic violence to the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of the law, if the individual agrees to the disclosure or to the extent that disclosure is expressly authorized by statute or

¹⁸⁵ 45 C.F.R. § 164.512(b) (2000).

¹⁸⁶ OCR Guidance Explaining Significant Aspects of Privacy Rule, Disclosures for Public Health Activities, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

¹⁸⁷ 45 C.F.R. § 164.512(b)(2) (2000).

regulation; and the covered entity believes the disclosure was necessary to prevent serious harm to the individual or other potential victims, or if the individual is unable to agree because of incapacity and the law enforcement officer or other public official authorized to receive the report represents that the protected health information for which disclosure sought is not intended to be used against the individual and an immediate enforcement activity depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to a disclosure.¹⁸⁸ Once such a disclosure is made, the individual must be promptly informed that the report was made or will be made, unless the covered entity believes that informing the individual will place the individual at risk of serious harm or that the covered entity will be informing a personal representative and the covered entity has reason to believe that the personal representative is responsible for the abuse, neglect, or other injury and informing the person would not be in the best interest of the individual.¹⁸⁹

- D. Disclosures for Health Oversight Activities. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law including audits, civil, administrative or criminal investigations, inspections, licensure or disciplinary actions, civil, administrative or criminal proceedings or actions or other activities necessary for the appropriate oversight of the health care system, government benefit programs for which health benefit information is relevant to beneficiary eligibility and is subject to government regulatory programs for which health information is necessary for determining compliance with program standards or is subject to civil rights law for which health information is necessary for determining compliance. However, an oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity, and such investigation or other activity does not arise out of and is not directly related to the receipt of health care, a claim for public benefits related to health, or a qualification for receipt of public benefits or services.¹⁹⁰
- E. Disclosures for a Judicial and Administrative Proceedings. The covered entity may disclose protected health information in the course of a judicial or administrative proceeding, in response to an order of the Court, administrative tribunal, subpoena, discovery request, or for all other purposes, if the entity receives satisfactory assurance from the party seeking disclosure that it made efforts to ensure the person who is the subject of the protected health information that has been requested, has been given notice of the request or receives satisfactory assurance from the person seeking the information that reasonable efforts have been made to secure a qualified protective order that meets the requirements of the regulations.¹⁹¹ The district court

¹⁸⁸ 45 C.F.R. § 164.512(c) (2000).

¹⁸⁹ 45 C.F.R. § 164.512(c) (2000).

¹⁹⁰ 45 C.F.R. § 164.512(d) (2000).

¹⁹¹ 45 C.F.R. § 164.512(e); *Biedrzycki v. Town of Cicero*, 2005 U.S. Dist. LEXIS 16423 (N.D. Ill. 2005) (approving disclosure pursuant to a qualified protective order).

for the Northern District of California held (citing 164.508(e) but describing the provisions in 45 CFR § 164.512(e) regarding disclosures permitted pursuant to judicial or administrative proceedings), that the defendant's right to privacy under the California Constitution did not outweigh the plaintiff's need for the defendant's medical records when the defendant's medical condition was an issue, thus the defendant was compelled to produce the records where an adequate protective order was already in place.¹⁹² The Internal Revenue Service indicated in a Chief Counsel Notice¹⁹³ that HIPAA's privacy regulations did not prevent the Internal Revenue Service (the "Service") from auditing a covered entity or a business associate of a covered entity, nor did it preclude such entities from responding since three exceptions permit the Service to obtain PHI, consent of the individual whose information is held by the taxpayer, the law enforcement exception and the administrative and judicial proceedings exception.

F. Disclosures for Law Enforcement Purposes. A covered entity may make a disclosure for law enforcement purposes to a law enforcement official if one of the following six requirements are met.

1. Disclosures Required by Law. The disclosure is required by law including laws reporting certain types of wounds or other physical injuries except this does not include reporting to the public health authority or government authority authorized to receive reports of child abuse, neglect or domestic violence, or reports of victims of abuse and neglect, or domestic violence.¹⁹⁴ The regulations define "required by law" to be a mandate on an entity.¹⁹⁵
2. Disclosure Pursuant to Order, Warrant, Subpoena, etc. The disclosure must be in compliance with and limited by the relevant requirements of the order, warrant, subpoena, summons, grand jury subpoena or administrative request including administrative subpoena or summons. The information sought must be relevant and material to legitimate law enforcement inquiry. The request must be specific and limited in scope to the extent reasonably practicable and de-identified information cannot be reasonably used. Disclosure to law enforcement can be for the purposes of identifying or locating a suspect, fugitive, material witness, or the missing person provided that the only information disclosed is the following: name, address, date and place of birth, social security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death (if applicable), and description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair,

¹⁹² *Hutton v. City of Martinez*, 2003 U.S. Dist. LEXIS 19852 (N.D. Ca. 2003).

¹⁹³ Chief Counsel Notice CC-2004-034 (Sept. 10, 2004).

¹⁹⁴ 45 C.F.R. § 164.512(f)(1) (2000).

¹⁹⁵ 45 C.F.R. § 164.103 (2003).

scars and tattoos. However, a covered entity may not disclose any protected health information related to the individual's DNA or DNA analysis, dental records, typing of samples or analysis of body fluids or tissue.¹⁹⁶

3. Disclosures of Limited Information for Identification and Location Purposes. A covered entity, if requested by a law enforcement official for purposes of identifying or locating a suspect, fugitive, material witness, or missing person may disclose an individual's name and address, date and place of birth, social security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death and a description of distinguishing physical characteristics. The covered entity may not disclose for purposes of identification any information related to an individual's DNA, DNA analysis, dental records or typing, samples or analysis of body fluids or tissue.¹⁹⁷
4. Disclosures Regarding Victims or Suspected Victims of Crimes. The covered entity may disclose health information about an individual who is or is suspected of being a victim of a crime if the individual agrees to the disclosure, or if you are unable to obtain the individual's agreement because of incapacity or other emergency circumstances, provided that the law enforcement official represents such information is needed to determine whether a violation of law by a person other than the victim has occurred, such information is not intended to be used against the victim, the official represents that the immediate law enforcement activity which depends on disclosure would be materially and adversely affected by waiting until the individual is able to agree to disclosure, and the disclosure is in the best interest of the individual, as determined by the covered entity.¹⁹⁸
5. Decedents. The covered entity may disclose protected health information about an individual who has died to a law enforcement official for alerting law enforcement of the death of the individual if there is a suspicion that the death may have resulted from criminal conduct.¹⁹⁹
6. Crime on the Premises. The covered entity can disclose protected health information that it believes, in good faith, constitutes evidence of a criminal conduct which occurred on the premises of the covered entity.²⁰⁰

¹⁹⁶ 45 C.F.R. § 164.512(f)(1)(ii) (2000).

¹⁹⁷ 45 C.F.R. § 164.512(f)(2) (2000).

¹⁹⁸ 45 C.F.R. § 164.512(f)(3) (2000).

¹⁹⁹ 45 C.F.R. § 164.512(f)(4) (2000).

²⁰⁰ 45 C.F.R. § 164.512(f)(5) (2000).

7. Reporting Crime in Emergencies. The covered health care provider providing emergency health care in response to a medical emergency may disclose protected health information to a law enforcement official after disclosure appears necessary to alert law enforcement to commission of a crime, the nature of a crime, the location of the crime or victim of such crime, and the identity, description and location of the perpetrator of the crime. However, if the health care provider believes that the medical emergency is the result of abuse, neglect, or domestic violence of the individual receiving the emergency health care, this disclosure for reporting crimes and emergencies does not apply.²⁰¹
- G. Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes. The covered entity may use or disclose protected health information to an organ procurement organizations or other entities that engage in procurement, banking, or transplantation of cadaveric organs, eye or tissue for the purposes of facilitating organ, eye or tissue transplantation.²⁰²
- H. Uses and Disclosures for Research Purposes. The covered entity may use or disclose protected health information for research, regardless of the sources of funding for the research, if there is an alteration to or waiver of the individual's authorization for use or disclosure of protected health information that is approved by either the institutional review board ("IRB") or a privacy board that meets the requirements of the regulations.²⁰³ Additional requirements apply to the use of research information and the privacy boards or IRB's. The proposed modifications made a number of changes to the waiver criteria for research.²⁰⁴
- I. Use or Disclosure to Avert a Serious Threat to Health or Safety. A use or a disclosure to avert a serious threat to health or safety are permitted disclosures provided all the requirements are met. A covered entity must in good faith believe that the disclosure is necessary to prevent or lesson a serious or imminent threat to the health or safety of the person or the public, and the disclosure must be made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat, or it must be necessary for law enforcement authorities to identify or apprehend the individual as a result of a statement made by the individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim, or where it appears from the circumstances that the individual has escaped from a correctional institution, or from lawful custody.²⁰⁵

²⁰¹ 45 C.F.R. § 164.512(f)(6) (2000).

²⁰² 45 C.F.R. §164.512(h) (2000).

²⁰³ 45 C.F.R. § 164.512(i) (2000).

²⁰⁴ 45 C.F.R. § 164.512(i)(2) (2002).

²⁰⁵ 45 C.F.R. § 164.512(j) (2000).

Use or disclosure of the protected information is not permitted, if the information is discovered in the course of treatment to effect the propensity to commit criminal conduct that is the basis for the disclosure or counseling or therapy or through a request by the individual to initiate or to be referred to treatment, counseling or therapy for treatment to affect the propensity to commit criminal conduct. A disclosure must only contain the statements made by the individual admitting participation in a violent crime, protected health information, such as the name, address, date of birth, place of birth, social security number, blood type-ABO and Rh factor, type of injury, date and time of treatment, etc. Any covered entity that uses or discloses the protected health information for this purpose is presumed to have acted in good faith with regard to their belief that the disclosure was needed to prevent serious threat to health or safety.²⁰⁶

J. Uses and Disclosures for Specialized Governmental Functions. These include use and disclosures for military and veterans activities, including activities deemed necessary by appropriate military command authorities to assure proper execution of the military mission. If there has been an appropriate authorization, or notice published in the Federal Register and the information is needed by components of the Department of Defense or Transportation it may be disclosed to the Department of Veterans Affairs for purposes of determining the eligibility or entitlement to benefits administered by the Secretary of Veterans Affairs, to health information for foreign military personnel, may be disclosed to their appropriate foreign military authority for purposes and uses that are permitted for United States personnel. Protected health information can be also disclosed to federal officials for the conduct of lawful intelligence, counter intelligence and other national security activities authorized by the National Security Act and the implementing authority to have the Executive Order 12333. It can also be disclosed to authorized federal officials for the provision of protective services to the President and other persons authorized by 18 U.S.C. 3056 or to foreign heads of states or for the conduct of investigation authorized by 18 U.S.C. 71 and 79. A covered entity that is part of the Department of State may use protected health information to make medical suitability determinations for limited purposes.

1. Correctional Institution. A covered entity may disclose to correctional institutions or law enforcement officials having lawful custody of an inmate protected health information about such inmate or individual, if the correctional institution or the law enforcement official represents that the protected health information is necessary for provision of health care to the individual, the health and safety of such individual or other inmates, the health and safety of the officers, employees or others at the correctional institution, in the health and safety of such officials and officers and other

²⁰⁶ 45 C.F.R. § 164.512(j) (2000).

persons responsible for transporting the inmate or the transfer from one institutional facility to another, for law enforcement on premises, for law enforcement on the premises of the correctional institution, and for the administration, maintenance of safety, security and good order of the correctional institution. The correctional institution may use the protected health information on inmates for any purposes for which such information may be disclosed. However, nothing may be disclosed after the individual is released on parole, probation, provisional release or is no longer in lawful custody.²⁰⁷

2. Governmental or Public Health Benefits. A health plan or government program providing public benefits may disclose protected health information according to eligibility for enrollment in the health plan to another agency, administering a government program providing public benefits if the sharing of the eligibility or enrollment information or maintenance of such information in a single or combined data system is accessible to all government agencies as required or expressly authorized by statute or regulations.²⁰⁸
3. Workers Compensation. A covered entity may disclose protected health information as authorized by, and to the extent necessary, to apply to the laws relating to workers compensation and similar programs established to provide benefits for work related injuries or illness without regard to fault.²⁰⁹ The privacy regulations generally do not apply to workers compensation insurers or administrative agencies or employers, except to the extent any of those are covered entities, such as the non-subscriber plans providing similar benefits as ERISA plans in Texas. The privacy regulations permit disclosures for workers compensation in a number of ways without authorizations, such as (1) for payment,²¹⁰ (2) to the extent disclosure is required by State or other law,²¹¹ or (3) as authorized by and to the extent necessary to comply with laws related to workers compensation or similar programs providing benefits without regard to fault.²¹² Disclosures can always be made with an individual's authorization. Disclosures for workers' compensation may be made to the full extent necessary as authorized by State or other law and it

²⁰⁷ 45 C.F.R. § 164.512(k)(5) (2000).

²⁰⁸ 45 C.F.R. § 164.512(k)(6) (2000).

²⁰⁹ 45 C.F.R. § 164.512(l) (2000).

²¹⁰ 45 C.F.R. § 164.502(a)(1)(ii) (2000).

²¹¹ 45 C.F.R. § 164.512(a) (2000).

²¹² 45 C.F.R. § 164.512(l) (2000).

will be subject to the minimum necessary standard because such requirement does not apply to disclosures required by State or other law.²¹³

- K. Uses and Disclosures for Fundraising. A covered entity may use and disclose to a business associate or to an institutionally related foundation the demographic information related to the individual and dates of health care provided to the individual for purposes of raising funds for its own benefit without receiving an authorization. The entity may not use or disclose protected health information for fund-raising purposes, unless, a statement about the use or disclosure is included in the covered entity's notice of privacy practices. The covered entity must include in any fundraising material it sends out to the individual, a description of how the individual may opt out of receiving any future fundraising communications.²¹⁴
- L. Uses and Disclosures for Underwriting and Related Purposes. The health plan may receive protected health information for purposes of underwriting, premium rating, and other activities related to the creation, renewal and replacement of contracted health insurance or health benefits. If such benefit program is not placed with the health plan receiving the information, then the health plan may not use or disclose such protected health information for any other purposes, except as may be required by law.²¹⁵

VI. Other Requirements Relating to Uses and Disclosures.

- A. De-Identified Protected Health Information. De-identified health information that has been de-identified in compliance with the regulations and for which there is no reasonable basis to believe that it can be used to identify an individual is not individually identifiable health information.²¹⁶ In order for the health information to be de-identified in compliance with the regulations, the covered entity may determine that the individually identifiable health information has been de-identified only if either: (1) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, applying those principles and methods, determines that the risk is very small that the information could be used alone or in combination with other reasonably available information to identify an individual who is the subject of the information, and the statistical person documents the methods and results of analysis that justify the determination, or (2) the information is de-identified using the regulation's safe harbor by deleting all of the following identifiers of the individual or relatives, employers or household members of the individual are

²¹³ OCR Guidance Explaining Significant Aspects of Privacy Rule, Workers' Compensation, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

²¹⁴ 45 C.F.R. § 164.514(f) (2000).

²¹⁵ 45 C.F.R. § 164.514(g) (2000).

²¹⁶ 45 C.F.R. § 164.514(a) (2000).

removed: names, all geographic subdivisions smaller than a state including street, address, city, county, precinct, zip code and the equivalent geo code, except for the three digits of the zip code can be maintained if the geographic unit formed by combining all the zip codes within the same three initial digits contains more than 20,000 people and the initial three digits of zip codes for all other geographic units containing 20,000 or fewer people are changed to 000. All elements of dates, except year for dates directly related to an individual including birth date, admission date, discharge date, date of death and all ages over 89 are all elements of dates including years indicative of such age are deleted, except that ages and elements may be aggregated into a single category of age 90 and older. All telephone numbers, fax numbers, electronic mail address, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identification and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locaters (URLs), internet protocol address numbers (IPs), biometric identifiers including finger and voice prints, photographic images, and other comparable images and any other unique identifying member, characteristic or code are deleted, except codes attached for reidentification.²¹⁷ The covered entity must not have any actual knowledge that the information could be used alone or in combination with other information to identify an individual whose information is included in the information. The covered entity can reassign codes to permit re-identification of the individuals following de-identification, as long as the code is not derived from or related to information about the individual and is not capable of being translated to identify the information, and the covered entity does not use or disclose the code as means of re-identification for any purposes.²¹⁸

- B. Uses and Disclosures of Protected Health Information for Marketing. The modifications deleted this portion of the regulations and reserved the location of the provision.²¹⁹ The final modifications used this area to insert the provisions governing use and disclosure of a limited data.²²⁰

VII. Disclosures in Litigation.

- A. General Guidelines. Disclosure issues frequently arise in many types of litigation. When litigation requires a covered entity to disclose PHI, careful reference should be made to 45 C.F.R. § 164.512(e) for the various basis for disclosure. Items B and C below will describe some of the bases for disclosure in judicial and administrative proceedings. It is important for covered entities to remember to obtain business

²¹⁷ 45 C.F.R. § 164.514(b)(2) (2002).

²¹⁸ 45 C.F.R. § 164.514(b) and (c) (2000).

²¹⁹ 45 C.F.R. § 164.514(e) (2000) was removed by the modifications.

²²⁰ 45 C.F.R. § 164.514(e) (2002).

associate agreements with their attorneys representing them in litigation before they provide PHI to their attorney.

- B. Pursuant to an Order of a Court or Administrative Proceeding. If the covered entity receives an order of a court or an administrative tribunal, it may disclose PHI pursuant to such an order, provided the covered entity discloses only the PHI expressly authorized by the order.²²¹
- C. Responding to Subpoenas, Discovery Requests or Other Lawful Processes That Are Not Accompanied by an Order of a Court or Administrative Tribunal. When a subpoena, discovery request or other lawful process requests PHI, but is not accompanied by an order from a court or administrative tribunal, the covered entity or its business associate attorney may disclose the PHI if either 1 or 2 below is satisfied:
1. The covered entity receives satisfactory assurances from the party seeking the information that the party seeking the information made reasonable efforts to ensure that the individual who is the subject of the PHI was given notice of the request. Satisfactory assurances for this purpose exist if the covered entity receives from such party a written statement and accompanying documentation that demonstrates:
 - a. the party requesting the information made a good faith attempt to provide written notice to the individual (or if the individual's location is unknown, to mail a notice to the individual's last known address); and
 - b. the notice contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
 - c. the time to raise objections has elapsed, and
 - (1) no objections were filed; or
 - (2) all objections filed were resolved by the court or administrative tribunal and the disclosures sought are consistent with such resolutions.²²²

A covered entity may disclose PHI without the above satisfactory assurances if the covered entity makes reasonable efforts to provide the individual the

²²¹ 45 C.F.R. § 164.512(e)(1)(i) (2000).

²²² 45 C.F.R. § 164.512(e)(1)(ii)(A) and (e)(1)(iii) (2000).

notice described above, or sought a qualified protective order as described below.²²³

2. The covered entity receives satisfactory assurances in the form of a written statement and accompanying documentation that demonstrates (A) the parties have either agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or (B) the party seeking the PHI has requested a qualified protective order from the court or administrative tribunal.²²⁴ The qualified protective order for this purpose must be an order of a court or administrative tribunal or stipulation of the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which it was requested and requires the PHI either be returned to the covered entity or destroyed (including all copies) at the end of the litigation or proceeding.²²⁵ If any attorney representing a covered entity in litigation receives protected health information, the attorney must consider his ethical obligations, requirements of his malpractice coverage and his firm's policies on file retention and the business associate agreement with the client before entering into a qualified protective order that requires him to destroy the records at the end of the proceeding. Business associate agreements can contain different language. A qualified protective order is issued by a court.²²⁶ Orders that do not protect the confidential information are not qualified protective orders.²²⁷

VIII. New Disclosure Procedures and Restrictions.

- A. General Standards Minimum Necessary - Access Limited Within Covered Entity. The covered entity must generally reasonably insure that all the requirements regarding use and disclosure for any particular request for disclosure are satisfied by the minimum amount of protected health information. Each covered entity must identify the persons or classes of persons in their work force who need access to protected health information to carry out their duties and for each person or class of persons, and the categories of protected health information to which each must have access and any conditions on such access. Each covered entity must make reasonable efforts to limit the access of such persons or classes to just the protected health information they need to be able to access.

²²³ 45 C.F.R. § 164.512(e)(1)(vi) (2000).

²²⁴ 45 C.F.R. § 164.512(e)(1)(ii)(B)(iv) (2004).

²²⁵ 45 C.F.R. § 164.512(e)(1)(v) (2000).

²²⁶ *Equal Employment Opportunity Commission v. Boston Market Corp.*, 2004 U.S. Dist. LEXIS 27338 (E.D.N.Y. 2004).

²²⁷ *Crenshaw v. MONY Life Insurance Company*, 318 F. Supp.2d 1015 (S.D. Ca. 2004).

For any type of disclosure that the covered entity may make on a routine and recurring basis, the covered entity must implement policies and procedures to limit the protected health information disclosed to the amount necessary to achieve the purposes of the disclosure. For all the disclosures, the covered entity must develop criteria designed to limit the information disclosed to that necessary to accomplish the purpose for which disclosure is sought, and review requests for disclosure on an individual basis in accordance with those criteria.²²⁸

For a group health plan, this means the group health plan must identify who has access and who must have access to protected health information and how much information each needs to be able to access. A group health plan must develop procedures for routine and recurring requests (e.g., coordination of benefits or subrogation) to limit the disclosure to the minimally necessary.²²⁹ The Office for Civil Rights has indicated that while entities must limit access of individuals based on their roles in the entity, that it does not necessarily consider facility redesigns as necessary, but that entities may need to make certain adjustments to facilities to minimize access, such as locking file cabinets or record rooms, or additional security, such as passwords on computers or software systems that contain protected health information.²³⁰

A covered entity may rely on the public official's statement that the request is limited to the minimum necessary when it is making disclosures to public officials that are permitted as uses or disclosures for which authorization or opportunity to agree or object are not required, or for those required by law for public health oversight, health activities or regarding victims of abuse or neglect or domestic violence, for judicial and administrative and law enforcement purposes, with respect to decedents, transplants and donors, and for specialized government functions. The covered entity may rely on a statement that the disclosure is the minimum necessary if the disclosure is requested by another covered entity,²³¹ or if it is requested by a professional who is a member of the work force or a business associate of a covered entity for purposes of providing professional services to the covered entity, if the professional represents it is minimally necessary. Any documents or representations that comply with the requirements for the research disclosure provided by a person requesting this information for research purposes satisfy the minimally necessary requirement.²³²

²²⁸ 45 C.F.R. § 164.514(d) (2000).

²²⁹ 45 C.F.R. § 164.514(d)(4)(iii) (2002).

²³⁰ OCR Guidance Explaining Significant Aspects of Privacy Rule, Minimum Necessary, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

²³¹ OCR Guidance Explaining Significant Aspects of Privacy Rule, Minimum Necessary, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

²³² 45 C.F.R. § 164.514(d) (2000).

- B. Verification Must Be Made Before Disclosure. Before any disclosure, the covered entity must verify the identity of the person requesting protected health information and the authority of the individual to have access to the information if the identity or authority is not known, and obtain any documentation, statements or representation, whether oral or written, from the person requesting the information when the documentation or statement of representation is a condition of the disclosure under the regulations. If a disclosure is conditioned on a particular documentation, statements or representations from the person requesting the information, the covered entity may rely on documentation or representations that on their face meet the applicable requirements if the reliance is reasonable, as explained in the regulations.²³³

IX. New Notice and Administrative Procedure Requirements Under the Privacy Regulations.

- A. Notice of Privacy Practices for Protected Health Information. An individual has a right to receive an adequate notice of the uses and disclosures of protected health information that may be made by a covered identity and the individual's rights and the covered entities legal duties with respect to protected health information. There is an exception for group health plans.
1. Self Insured or Partially Self Insured Plans. An individual who is enrolled in group health plan has a right to receive the notice from the group health plan if the individual does not receive health benefits under the group health plan through an insurance contract or health insurance issuer or HMO. Such a group health plan must also comply with a number of additional standards to implement the privacy regulations, including, designating a privacy contact or office to receive complaints, designating and training all personnel to handle PHI with respect to the privacy policies and procedures, establishing safeguards to protect the PHI, establishing a process for handling complaints related to misuse of PHI and documenting such complaints, establishing sanctions against its personnel who fail to comply with the privacy policies and procedures, and documenting the sanctions imposed, establishing a standard to mitigate any harm from a disclosure in violation of the regulations, refraining from intimidation or retaliatory acts, provide a standard that it does not require individuals to waive their rights, establishing policies and procedures on privacy and documentation of the same, and documenting all communications, actions, or activities required by the regulations.²³⁴
 2. Fully Insured Group Health Plan or HMO and Plan Receives More Than Summary Health Information. If a group health plan provides health benefits

²³³ 45 C.F.R. § 164.514(h) (2000).

²³⁴ 45 C.F.R. § 164.520(a)(2) (2000) and 45 C.F.R. § 164.530 (2000).

solely through an insurance contract with a health insurance issuer or HMO, and the group health plan creates or receives protected health information in a format other than either summary health information or information on whether the individual is participating in the group health plan or is enrolled or disenrolled from the health insurance issuer or HMO offered by the plan, the plan must maintain a privacy practices notice and provide the notice upon request to any person.²³⁵ The insurer or HMO would still have the obligation to provide the privacy notice. Such a group health plan must also comply with a number of additional standards to implement the privacy regulations, including, designating a privacy contact or office to receive complaints, designating and training all personnel to handle PHI with respect to the privacy policies and procedures, establishing safeguards to protect the PHI, establishing a process for handling complaints related to misuse of PHI and documenting such complaints, establishing sanctions against its personnel who fail to comply with the privacy policies and procedures and documenting that the sanctions are imposed, establishing a standard to mitigate any harm from a disclosure in violation of the regulations, refraining from intimidation or retaliatory acts, provide a standard that it does not require individuals to waive their rights, establishing policies and procedures on privacy and documentation procedures for policies, procedures and documenting all communications, actions, or activities required by the regulations.²³⁶

3. Fully Insured or HMO and Protected Information Only Received in Summary Format or Not at All. If the group health plan provides health benefits solely through an insurance contract with the health insurance issuer or HMO and does not create or receive protected health information other than in the form of summary health information, de-identified health information, or information on whether the individual is participating or is enrolled in or has disenrolled from the health insurance issuer or HMO offered by the plan, the health plan is not required to maintain or provide a notice under the regulations.²³⁷ Such plans must only comply with the standards for refraining from intimidating or retaliatory acts and the standards for waiver of rights.²³⁸
4. Correctional Institution Plans. Inmates do not have a right to a notice. The notice requirements do not apply to a correctional institution that is a covered entity.²³⁹

²³⁵ 45 C.F.R. § 164.520(a) (2000).

²³⁶ 45 C.F.R. § 164.520(a)(2) (2000) and 45 C.F.R. § 164.530 (2000).

²³⁷ 45 C.F.R. § 164.520(a) (2000).

²³⁸ 45 C.F.R. § 164.530(k) (2000).

²³⁹ 45 C.F.R. § 164.520(a) (2000).

- B. Notice Contents. The notice must include a certain content. The notice must have the following header:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

The notice must also contain a description, that includes at least one example, of the types and uses of disclosures that the entity is permitted to make by the privacy regulations to make for each of the following purposes of the treatment, payment and health care operations. The notice must contain a description of how each of the other purposes for which the covered entity is permitted or required by the privacy regulations to use or disclose the protected health information without the individual's written consent or authorization. If one of the uses or disclosures described above is prohibited or materially limited by other applicable laws, description of such use and disclosure must reflect the more stringent law. The description must have sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by the privacy regulations and other applicable laws. The notice must have a statement that any other uses or disclosures will be made only with the individual's written authorization. There must be a statement that the individual may revoke such authorization in writing.²⁴⁰ ERISA preemption of state laws imposing state law health plan privacy requirements on a health plan is particularly important for employers operating in multiple states to avoid the need to analyze each state's medical privacy laws and whether or not they are more stringent or not, and to more importantly avoid making the privacy notice for the health plan into a multi-volume discussion of state laws.

If the covered entity intends to engage in any of the activities listed below, the notice must include a separate statement that the entity (a) may contact the individual to provide appointment reminders for information about treatment alternatives or other health related benefits and services, (b) that the entity may contact the individual to raise funds for the covered entity, and (c) that the group health or health insurance issuer or HMO may disclose protected health information to the sponsor of the plan.²⁴¹

A notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise those rights including the right to request restrictions on certain uses and disclosures of protected health information, the right to receive confidential communication of protected health information, the right to inspect and copy protected health

²⁴⁰ 45 C.F.R. § 164.520 (2000).

²⁴¹ 45 C.F.R. § 164.520(b) (2000).

information, the right to amend protected health information, the right to receive an accounting of disclosures of protected health information, the right of an individual to obtain a paper copy of the notice from the covered entity upon request if the individual previously agreed to receive the notice electronically. That notice must also contain a statement of covered entity that is required by law to maintain the privacy of protected health information and provide the individual with notice of its legal duties and privacy practice with respect to the information. A statement that the covered entity is required to abide by the terms of the notice currently in effect and that if the covered entity desires to change its policies that in order to apply a change in the privacy practice that is described in the notice to protected health information, the covered entity created or received prior to issuing a revised notice, the notice must include a statement that it reserves the right to change the terms of its notice and to make new notice provisions effective for all protected health information that it maintains. A notice must also describe how the individuals will receive a revised notice.²⁴²

There must be a statement regarding complaints and how the individual may complain to the covered entity and to the secretary of HHS if they believe their privacy rights were violated including a description of how to file a complaint and a statement that the individual will not be retaliated against for filing a complaint.²⁴³

The notice must include the name, title, or telephone number of a person or office to contact for further information. The notice must contain the date in which the notice is first in effect and may not be earlier than the date in which the notice is printed or otherwise published.²⁴⁴

If the covered entity decides to limit a use or disclosure that it is permitted to make under the regulations, the covered entity may describe its more limited use or disclosure policy in the notice. However, the covered entity may not include in its notice a limitation affecting its rights to make a use or disclosure that is required by law or permitted to prevent or lessen a serious or imminent threat to the health and safety of a person or the public. If a covered entity decides to revise its notice, it may only do so if it has reserved the right to revise its practices and procedures in its previous privacy notice, stated that it may make the changes effective for all protected health information it maintains, and provides a notice whenever there is a material change to the uses or disclosures.²⁴⁵

The notice must be available to an individual upon request. A health plan must provide the notice no later than the compliance date for the health plan under the

²⁴² 45 C.F.R. § 164.520(b) (2000).

²⁴³ 45 C.F.R. § 164.520(b) (2000).

²⁴⁴ 45 C.F.R. § 164.520(b) (2000).

²⁴⁵ 45 C.F.R. § 164.520(b) (2000).

privacy regulations. Thereafter, it must be provided at the time of enrollment to individuals who are new enrollees and within sixty days of any material revision to the notice. It also must be provided no less than frequently than once every three years, unless individuals then covered under the plan are notified of the availability of the notice and how to obtain the notice. The notice requirements are satisfied if they provide to the named insured under the policy. Health care providers must provide the notice at the first service delivery. After the compliance date for the health care providers, the health care provider must have the notice available at the service delivery site for individuals to request to take with them and the health care provider must post the notice in a clear and prominent location where it is reasonable to expect individuals obtaining service from the covered health care provider to be able to read the notice. It must make new notices available whenever there is a revision. There is a provision provided for electronic notices and for joint notices from separate entities.²⁴⁶

- C. Individuals May Request Restrictions on Access. An individual may request that the covered entity restrict the uses and disclosures of protected health information only to the person who will carry out treatment, payment and health care operations, disclosures that give the individual an opportunity to agree or to object to the disclosure and use to individuals that are involved in the individual's care and to a public or private entity when disclosure is authorized by law or its charter to assist in disaster relief efforts. However, a covered entity is not required to agree to such a restriction. If a covered entity does permit the creation of a restriction, they must abide by the restrictions. Any restriction cannot be used to prevent disclosure for facility directories, disclosures to an individual when requested by the individual for their own purposes or disclosure for which authorization or an opportunity to agree or object is not required. A covered entity may terminate its agreement to a restriction, if the individual agrees to the termination request in writing. If the individual orally agrees to terminate the restriction and the oral agreement is documented, or the covered entity informs the individual that it is terminating its agreement to a restriction, the restriction may be terminated. The termination of the restriction is only effective with respect to information created or received after the individual is informed and agrees to the termination.²⁴⁷
- D. Access to the Individual. Individuals must have a right to access to obtain a copy of their protected health information for all information except (a) psychotherapy notes, (b) information compiled in a reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding, and (c) protected health information that is subject to the Clinical Laboratory Improvements Act of 1988 to the extent the provision of the access to the individual would be prohibited by law or information that is exempt from the Clinical Laboratory Improvements Act of 1988. Covered

²⁴⁶ 45 C.F.R. § 164.520 (2000).

²⁴⁷ 45 C.F.R. § 164.522 (2000).

entities may deny an individual access to their records only in limited circumstances specified by the regulations. A covered entity that denies an individual the right to access their information must give the individual a right to have the denial reviewed by a licensed health care professional.²⁴⁸

Access may be denied in limited circumstances without review. Access may be denied with review for a request that (a) may endanger the life or physical safety of the individual or another person, (b) if the protected health information makes reference to another person and the access requested is reasonably likely to cause substantial harm to the other person, or (c) if the access requested is made by the individual's personal representative and the health care professional determines that the provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

Any denial of access may be reviewed by a licensed health care professional designated by the covered entity to act as the reviewing official who did not participate in the original decision to deny. Any request for access must be responded to no later than 30 days after it is received. If it is denied, there must be a written denial. If it is accepted, then the individual must be notified of the acceptance and provide the access requested. If the information is not on site, the entity may have 60 days to respond. If the entity is unable to take an action on a request within 30 days of receipt, it may extend the time for response by 30 days. Only one extension is permitted. The access must include inspection, copying or both. It must be provided in the form or format requested, if it is readily reducible in such form; if not, in a readable hard copy form. A summary of the information can be provided in place of the actual information if the individual agrees in advance to the summary and agrees to any fees imposed on preparation of the summary or explanation. A covered entity may impose a reasonable cost based fee for the copying, postage and preparation of any explanation or summary of the information. A covered entity must record and retain documentation regarding the information subject to access by the individuals and the titles of persons responsible for receiving and processing the request for access.²⁴⁹

- E. Right to Amend. An individual has the right to request a covered entity amend the protected health information or record about the individual that is maintained in a designated record set for the individual. A covered entity may deny an individual's request for amendment if the terms of the protected health information or record that is the subject of the request was not created by the covered entity, is not part of the designated record set, will not be available for inspection or is accurate and complete. The covered entity must have a procedure for handling a request to an amendment to the record. The individual must make the request in writing and provide a reason to

²⁴⁸ 45 C.F.R. § 164.524(a) (2000).

²⁴⁹ 45 C.F.R. § 164.524 (2000).

support the request for amendment. The covered entity must act within the same time frame for adjudicating a request to amend as a covered entity receiving a request for access to health information. Any denial of a request for amendment must state the basis for denying the amendment and indicate the individual's right to submit a written statement disagreeing with the denial and how the individual may file for such statement. It must include a provision for a description of the compliant procedure for the covered entity and the Secretary of HHS. The covered entity must permit the individual to submit a written statement disagreeing with denial of all or part of the requested amendment and basis of the disagreement and the covered entity may reasonably limit the length of the statement of the disagreement. The covered entity may include a written rebuttal to the participant's statement of disagreement. The covered entity must identify the record of protected health information, the designated record set, that is the subject of the disputed amendment and append or otherwise attach the individual's request for the amendment, the covered entity's denial, the individual's statement of disagreement and the entity's rebuttal to the designated record set. Any future disclosure must include all of the appendages as well. That information may be separately transmitted if it does not fit within the standard data code set.

The covered entity must document the titles of the persons or officers responsible for receiving and processing requests for amendments by individuals and retain the documents.²⁵⁰

- F. Right to Accounting of Disclosures. The covered entity must keep an accounting of all uses or disclosures of protected health information by the covered entity for the six years prior to the date on which the accounting is requested. The accounting for disclosures does not need to include the disclosures for carrying out treatment, payment or health care operations, to individuals of health information about themselves, pursuant to an authorization for psychotherapy notes or marketing, for the facility's directories, for the persons involved in the individual's care, for national security or intelligence purposes, to correctional institutions or law enforcement officials, that were incident to a use or disclosure otherwise required or permitted under the privacy regulations (required as provided in 45 C.F.R. § 164.502), disclosures that occurred prior to the compliance date of the covered entity or as part of a limited data set in compliance with the regulations.²⁵¹ The covered entity must temporarily suspend an individual's rights to receive an accounting of disclosures pursuant to a health oversight agency or law enforcement official's request at the time specified by the agency or official if the agency or official provides the covered entity with a written statement that the accounting to the individual would be likely to impede the agency's activities and specifies the time for which the suspension is required. The written accounting must be provided to the individual and must meet

²⁵⁰ 45 C.F.R. § 164.526 (2000).

²⁵¹ 45 C.F.R. § 164.528(a) (2002).

the following requirements to include disclosures of protected health information that occurred during the six years prior to the date of the request for the accounting, including disclosures to or by the business associates of the covered entity. This means business associates must keep records of any disclosures they make.²⁵²

The accounting for each disclosure must include the date of the disclosure, the name of the entity or person who received the information and the address of such entity or person, a brief description of the protected health information disclosed and a brief statement of the disclosure's purpose that reasonably informs the individual of the basis of the disclosure. A copy of the individual's written request for disclosure to the Secretary of HHS or disclosure where consent or authorization to agree or object is not required must be maintained and included in the accounting for disclosures. A special rule exists for multiple disclosures.²⁵³ If during the period of the accounting, the covered entity made a disclosure for a particular research purpose for 50 or more individuals, the accounting may provide the name of the protocol or research activity, a plain language description of the research, including its purpose, a brief description of the type of protected health information disclosed, the date or period during which the disclosure was made, the name, address and telephone number of the entity sponsoring the research and a statement that the individual's protected health information may or may not have been disclosed for the research activity. If it is reasonably likely that the individual's protected health information was disclosed for the research, if the individual requests, the covered entity must assist in contacting the entity that sponsored the research or the researcher.²⁵⁴

The accounting of the disclosure must be provided within 60 days of the receipt of the request for the accounting of disclosures. This may be extended for one time period for up to 30 days. Only one accounting must be provided to an individual in any 12 month period without charge.²⁵⁵ A covered entity may impose reasonable cost based fee for subsequent requests for accountings by the same individuals within the same 12 month period provided they notify the individual in advance of the fee and they give the individual an opportunity to withdraw or modify the request for the accounting.²⁵⁶

- G. Confidential Communications. A health care provider must abide by an individual's reasonable request for confidential communications at an alternate location or by an alternate means. Similarly, a health plan must also abide by such reasonable requests

²⁵² 45 C.F.R. § 164.528 (2000).

²⁵³ 45 C.F.R. § 164.528(b) (2002).

²⁵⁴ 45 C.F.R. § 164.528(b)(4) (2002).

²⁵⁵ 45 C.F.R. § 164.528(c)(2) (2000).

²⁵⁶ 45 C.F.R. § 164.528 (2000).

if the individual clearly states that the health plan's failure to comply could endanger the individual.²⁵⁷

- H. Procedures to be Implemented by Covered Entities. Each covered entity must designate a privacy official responsible for development and implementation of the policies and procedures of the entity and also a contact person or office responsible for receiving complaints and who can provide further information.²⁵⁸

The covered entity must train all members of the work force on the policies and procedures with respect to protected health information necessary for the work force to carry out their function within the entity. The training must meet the requirements of the regulations, it must be provided to each member of the work force no later than the compliance date for the covered entity and to each new member of the work force within a reasonable period of time after joining the work force and to each member of the covered entity's work force whose functions are affected by material changes in policies or procedures within a reasonable period of time after those policies or procedures become changes become effective. The covered entity must document the training.²⁵⁹

The entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.²⁶⁰ The covered entity must reasonably safeguard and protect health information from intentional or unintentional use or disclosure in violation of the privacy requirements. The covered entity must provide the process for individuals to make complaints concerning the covered entity's policies and procedures regarding privacy.²⁶¹

The covered entity must have and apply appropriate sanctions against members of the work force who have failed to comply with the privacy policies and procedures. They must document the sanctions applied. The covered entity must mitigate any harmful effect that is known to it for of the use or disclosure of protected information in violation of the privacy requirements.²⁶²

The covered entity may not intimidate, threaten or coerce, discriminate against or take any retaliatory action against an individual for the exercise of their rights under

²⁵⁷ 45 C.F.R. §§ 164.502(h) and 164.522(b) (2000); OCR Guidance Explaining Significant Aspects of the Privacy Rule, Uses and Disclosures for Treatment, Payment and Health Care Operations, found at www.hhs.gov/ocr/hipaa/privacy.html, Dec. 4, 2002.

²⁵⁸ 45 C.F.R. § 164.530(a) (2000).

²⁵⁹ 45 C.F.R. § 164.530(b) (2000).

²⁶⁰ 45 C.F.R. § 164.530(c) (2000).

²⁶¹ 45 C.F.R. § 164.530(d) (2000).

²⁶² 45 C.F.R. § 164.530(e) and (f) (2000).

the privacy regulations or filing a complaint with the Secretary for testifying or assisting or participating in an investigation or compliance review of the Secretary or for opposing any act or practice made unlawful by the privacy regulations, if they have a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable.²⁶³

The covered entity may not require individuals to waive their rights to make complaints to the Secretary of HHS that the condition or provision of treatment, payment and enrollment in the health plan or eligibility for benefits.²⁶⁴

The covered entity must implement policies and procedures with respect to protected health information which are designed to comply with the privacy regulation standards and those policies and procedures must be reasonably designed to take into account the size and type of the activities that relate to protected health information undertaken by the entity to ensure compliance.²⁶⁵

The covered entity must change its privacy policies and procedures to keep in compliance with the law. If there is a change in the privacy policy and procedures they must change the notice and provide the changed notice to in compliance with the notice requirements in 45 C.F.R. § 164.520.

- I. Effective Date. The compliance date for small health plans with less than \$5,000,000 in receipts was originally February 26, 2004, and was delayed to April 14, 2004. For health plans that are not small health plans, the compliance date was originally February 26, 2003, and was delayed to April 14, 2003. Health care providers and health care clearinghouses originally were required to comply by February 26, 2003, and this was delayed to April 14, 2003.²⁶⁶ There was no provision for an effective date with respect to plan years beginning on or after a certain date; thus, the privacy provisions became effective mid-plan year for most plans, and required a mid-year amendment. The privacy regulations were used as an example demonstrating a strong federal policy of protection of patients' medical records and used to guide how records were to be disclosed in a federal criminal proceeding against a doctor for allegedly unlawfully dispensing drugs. The court required notice to the individuals who obtained the prescriptions with an opportunity to object prior to the disclosure.²⁶⁷

²⁶³ 45 C.F.R. § 164.530(g) (2000).

²⁶⁴ 45 C.F.R. § 164.530(h) (2000).

²⁶⁵ 45 C.F.R. § 164.530(i) (2000).

²⁶⁶ 45 C.F.R. § 164.534 (2000) and 65 F.R. 82944, and delayed by 66 F.R. 12433 (2001).

²⁶⁷ *U.S. v. Sutherland*, 2001 WL 497106, 143 F. Supp.2d 609 (W.D. Va. 2001).

- J. Transition Rule for Authorizations. Transition rules provide that previously received authorizations are still effective as long it permits the use or disclosure for purposes of carrying out treatment, payment or health care operations, or the purpose for which the information is to be used or disclosed and no agreed restriction that prohibits the disclosure.²⁶⁸ If a covered entity does not make any use or disclosure that is expressly excluded from the existing authorization and complies with all limitations in the consent or authorization, it generally complied with the transition rule.²⁶⁹ The transition rules in the proposed modifications purport to give a period of "deemed compliance" for any entity other than a small group health plan (receipts of less than \$5,000,000) with respect to its business associate agreements. However, in order to be in deemed compliance the contract must not be reviewed or modified from the effective date of the proposed modification until a date that is after April 14, 2003. The transition gives the covered entity until the contract's next renewal date or April 14, 2004, whichever is earlier; however, the covered entity still needed to comply with the requirements to give individuals access, the ability to amend and to provide an accounting of protected health information disclosures.²⁷⁰
- X. Enforcement of Privacy for Individually Identifiable Health Information. The health care information that is individually identifiable is also subject to additional protections.²⁷¹ Both a civil and a criminal enforcement mechanism exist to enforce the privacy regulations.
- A. Criminal Enforcement. Any person who knowingly and in violation of this part uses or causes to be used a unique health care identifier, obtains individually identifiable health information related to an individual, or discloses individually identifiable health information to another person may be fined not more than \$50,000 and imprisoned not more than one year or both. If the above offense is committed under false pretenses, the individual may be fined not more than \$100,000 and imprisoned not more than five years or both. If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the individual may be fined not more than \$250,000 or imprisoned not more than 10 years or both.²⁷² While late in 2004 an individual working in a health care clinic was convicted and sentenced to jail for using a patient's PHI in an identity theft, the U.S. Department of Justice issued an opinion on June 1, 2005,²⁷³ that indicated individual employees of covered entities are not directly subject to the criminal requirements of HIPAA privacy. The opinion stated only covered entities are subject to the criminal penalties for a violation of the

²⁶⁸ 45 C.F.R. § 164.530(a) and (b) (2002).

²⁶⁹ 45 C.F.R. § 164.532 (2000).

²⁷⁰ 45 C.F.R. § 164.532 (2002).

²⁷¹ 42 U.S.C. § 1177.

²⁷² 42 U.S.C. § 1177.

²⁷³ The opinion is found at www.usdoj.gov/olc/hipaa_final.htm.

HIPAA privacy regulations, and individuals, who are not covered entities themselves, can only be liable for a privacy violation if principles of corporate criminal liability attribute the violation to the individual. Principles of corporate criminal liability will determine when a covered entity has violated HIPAA privacy and when those violations can be attributed to individuals in the entity.²⁷⁴

- B. Civil Enforcement. A civil penalty is provided for each type of violation of \$100.00 per day per person up to \$25,000.00 per violation of a single standard in a single calendar year.²⁷⁵ There is no limit on the numbers of types of violations on which the civil penalty can be assessed. The Secretary of HHS may bring enforcement actions seeking to impose the civil monetary penalties. The Secretary of HHS may not institute an action for a civil monetary penalty later than six years after the date of the occurrence that is the basis for the penalty.²⁷⁶ A civil penalty can only be imposed after the individual is given written notice and an opportunity for a determination to be made on the record after a hearing at which the individual may be represented by his own counsel or by himself.²⁷⁷ The U.S. Department of Health and Human Services Office for Civil Rights ("OCR"), to the extent practicable, will seek cooperation in obtaining compliance with the Privacy Regulations.²⁷⁸ If an individual fails to respond and request a hearing within 60 days after receipt of a proposed determination,²⁷⁹ the Secretary must impose the proposed penalty or a less severe penalty.²⁸⁰ Once the penalty is imposed, it must be collected.²⁸¹ The individual can respond and request a hearing before an administrative law judge and the regulations or imposition of civil monetary penalties detail the procedural requirements for the hearing. The Secretary has the exclusive authority to settle any case or issue without the consent of the administrative law judge; thus, it is imperative that upon receipt of a notice of proposed determination the party respond within 60 days and begin addressing the issue.²⁸² The expiration date for the Interim Final Rule on Imposition of Civil Monetary Penalties for violations was again extended on September 14, 2005 to March 16, 2006.²⁸³ The final Civil Monetary Penalties regulation was issued on February 16, 2006, effective on March 16, 2006.²⁸⁴

²⁷⁴ *Id.*

²⁷⁵ 45 C.F.R. §§160.306 and 160.312 (2000).

²⁷⁶ 42 C.F.R. § 1320a-7a.

²⁷⁷ 68 F.R. 18895, 18896 (2003).

²⁷⁸ 68 F.R. 18895, 18897 (2003).

²⁷⁹ 45 C.F.R. § 160.514 (2003).

²⁸⁰ 45 C.F.R. § 160.516 (2003).

²⁸¹ 45 C.F.R. § 160.518 (2003).

²⁸² 45 C.F.R. § 160.536 (2003).

²⁸³ 70 Fed. Reg. 54293 (September 14, 2005).

²⁸⁴ 71 F.R. 8390 (February 16, 2006).

C. No Private Cause of Action. Private rights of actions are not authorized for disclosure violations, but individuals may report such disclosure violations to the Department of Health and Human Services, Office of Civil Rights.²⁸⁵ However, there may be an action under the Employee Retirement Income Security Act of 1974, as amended ("ERISA"), if the disclosure violates the privacy terms of a group health plan that is subject to ERISA. The incorporation of the privacy provisions in the plan document as required by the Privacy Regulations²⁸⁶ provides the participants the right to seek to enforce the terms of the plan document under section 502(a)(3) of ERISA. However, the remedy for seeking to enforce the plan's terms is limited to appropriate equitable relief and what exactly constitutes appropriate equitable relief remains to be determined following *Great-West Life & Annuity Ins. Co. v. Knudson*.²⁸⁷

XI. Security. Health plans, health care clearinghouses and health care providers who transmit any health information in an electronic form in connection with a standardized electronic claim transaction under section 1173(a)(1) of the Public Health Service Act must also implement security standards for health information to take into account the technical capabilities record systems, the costs of security, the need for training personnel with access to protected health information, and the need for audit trails in computerized record systems and the needs and capabilities of small and rural health care providers. The safeguards must provide reasonable and appropriate administrative, physical and technical safeguards to ensure the integrity and confidentiality of the health information and to protect against reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information and to ensure compliance by its officers and employees. See the separate outline on the final security regulations for further information.

XII. Privacy in Mergers, Acquisitions and Corporate Transactions.

A. Due Diligence.

The Privacy Regulations generally permit disclosures for treatment, payment and health care operations.²⁸⁸ Included in the definition of health care operations is:

²⁸⁵ *Slue v. New York University Medical Center*, 409 F. Supp. 2d 349 (S.D. N.Y. 2006); *Runkle v. Gonzalez*, 2005 U.S. Dist. LEXIS 22219 (D.O.C. 2005); *Protection & Advocacy System, Inc. v. Freudenthal*, 2006 U.S. Dist. LEXIS 3529 (D. Wyo. 2006); *Redtke v. American Federation of State, County and Municipal Employees – Milwaukee District Council 48*, 376 F. Supp. 2d 893 (E.D. Wis. 2005); *Haranzo v. The Department of Rehabilitative Services*, 2005 U.S. Dist. LEXIS 27302 (W.D. Va. 2005); *Johnson v. Milwaukee County*, 2006 U.S. Dist. LEXIS 6892 (E.D. Wis. 2006).

²⁸⁶ 45 C.F.R. § 164.504(f) (2003).

²⁸⁷ 534 U.S. 204, 112 S. Ct. 708, 151 L.Ed.2d 634 (2002).

²⁸⁸ 45 C.F.R. § 164.502(a)(i) and (ii) (2002).

"The sale, transfer, merger or consolidation of all or part of the covered entity with another covered entity, or an entity that will become a covered entity and due diligence related to such activity;"²⁸⁹
(Emphasis added.)

Thus, when two covered entities under the Privacy Regulations or an entity that will become a covered entity is involved in a corporate transaction, such as a pharmacy, then protected health information can be shared as part of the due diligence related to such activity. However, the sharing of the information must be by the covered entity that is a party to the transaction.²⁹⁰

However, when two entities that are merely plan sponsors of covered entities engage in a corporate transaction, there is no provision permitting disclosure of protected health information from the health plans sponsored by the entities engaged in the transaction. Thus in transactions in which plan sponsors merge or otherwise acquire or dispose of a trade or business or other corporate assets, until further guidance is issued, it appears that only de-identified information or summary health information or limited data sets may be exchanged between the plan sponsors.

The preamble to the final modifications to the final privacy regulations issued on August 14, 2002, provides that when covered entities merge, then the new owner may immediately use and disclose the records to provide health care services and for purposes of payment and health care operators, this assumes that it is a covered entity that is a party to the transaction.²⁹¹ This permits the covered entity that merges to immediately use protected health information in its treatment, payment and health care operations, but again, it does not extend to health plans sponsored by employers engaged in corporate transactions when the health plans themselves are not merged as part of the transaction. Frequently, the health plans are not merged when the corporate transaction occurs in order to permit less disruption to the employees, or because the nature of the corporate transaction did not result in the health plans under the control of one entity. However, in many asset sales the employees are transferred and cannot stay in the same plan and the new employer wants to make the transition to the new plan easier by crediting funds expended toward deductibles and limits in the old plan by the individual in the new employer's plan.

The preamble to the final modifications to the final Privacy Regulations further indicates that if a transaction is not consummated, standard business practices, such as confidentiality agreements that buyers and sellers typically enter into with regard

²⁸⁹ 45 C.F.R. § 164.501 (2002).

²⁹⁰ 67 F.R. 53182, 53190 (August 14, 2003).

²⁹¹ 67 F.R. 53182, 53190 (2002).

to proprietary information, are sufficient to ensure that the health information transferred is either returned to the original owner or destroyed.²⁹²

However, the preamble's comment is in the context of sharing of protected health information between two covered entities or an entity that will become a covered entity after the corporate transaction and does not provide guidance regarding corporate transactions between non-covered entities that sponsor group health plans. Given that the Privacy Regulations do not expressly address the situations arising when non-covered entities that sponsor covered entities engage in corporate transactions that do not result in the group health plans merging concurrently with the corporate transaction or at a later time, the Privacy Regulations do not currently permit the plan sponsors to cause the group health plans to provide protected health information to the other plan sponsor or group health plan absent an authorization from each covered person. Thus, due diligence can only be completed by using de-identified information, summary health information, or by entering into a business associate agreement with an independent third party to perform health care operations or payment with regard to the plan (such as ceding new coverage) who will analyze the data and provide de-identified information or a report on such analysis to the other party.

B. Plan Transition Issues.

When a corporate transaction occurs between two group health plan sponsors that does not result in the two group health plans merging, frequently the plan sponsors will want to protect the employees by preserving their status in health flexible spending accounts and in the group health plan with respect to amounts satisfied toward deductibles, out-of-pocket maximums or other limits so that they are not required to satisfy those amounts in two plans in the same year as the result of the corporate transaction. While no guidance directly addresses the disclosure or use of the information for such purposes, the definition of health care operations reads:

"(3) Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits and ceding, securing or placing a contract for reinsurance of risk for health care."²⁹³

and of the definition of payment reads:

"(1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan;"

²⁹² 67 F.R. 53182, 53191 (2002).

²⁹³ 45 C.F.R. § 164.501 (2002).

may provide some argument for transferring information from one group health plan to another to facilitate replacement of a contract of health benefits or in order to fulfill its responsibility for coverage and provision of benefits under the health plan.

The disclosures of protected health information by the prior plan to the new plan and the use of such information by the successor plan arguably falls within these definitions when interpreted broadly; however, there is no explicit indication such use or disclosure was intended or contemplated. Such use or disclosure would further the goal of not having the Privacy Regulations disrupt the operation of group health plans in the provision of benefits or in the payment for delivering health care; however, it is not clear this use or disclosure is covered or intended since it was not explicitly dealt with when covered entity mergers were addressed.

D-1190027.7