TABLE OF CONTENTS

HIPAA PRIVACY RULE SUMMARY

An "unofficial" version of the modified Final Privacy Rule can be accessed at:
http://www.hhs/gov.ocr/combinedregtext.pdf
Additional information on the HIPAA Privacy Rule can be accessed at:
http://www.hhs.gov/ocr/hipaa/

INTRODUCTION AND OVERVIEW OF AUGUST 2002 MODIFICATIONS:

Background: The Health Insurance Portability and Accountability Act of 1996 (HIPAA), public law 104-191, relates in part to health information privacy issues with these issues being regulated through federal regulations by the United States Department of Health and Human Services (HHS). HHS published the regulation in the form of a privacy rule in December 2000. In August 2002 HHS adopted as a final rule modifications made to the December 2000 privacy rule.

HHS December 2002 Guidance: On December 3, 2002 the Office for Civil Rights (OCR), the enforcement arm of HHS with responsibility for enforcement of the HIPAA privacy rule issued a 123-page guidance interpreting and applying the August 2002/December 2000 HIPAA privacy rule.

Included within the December 3, 2002 guidance is the explanation that the HIPAA privacy rule requires "activities" such as:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or health plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them. (OCR HIPAA privacy guidance, December 3, 2002, page 5).

The OCR guidance recognizes that the privacy rule "gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs." Additionally, the guidance indicates the "scalability of the [privacy] Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard." (OCR HIPAA privacy guidance, December 3, 2002, page 6).

August 2002 Modifications from December 2000 Rule: Major modifications were made to the HIPAA privacy rule in August 2002. HHS has summarized these "major modifications" as follows:

> Based on the information received through public comment, testimony at public hearings, meetings at the request of the industry and other stakeholders, as well as other communications, HHS identified a number of areas in which the Privacy Rule, as issued in December 2000, would have had potential unintended effects on health care quality or access. As a result, HHS proposed modifications that would maintain strong protections for the privacy of individually identifiable health information, address the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieve unintended administrative burdens created by the Privacy Rule.
>
> Final modifications to the Rule were adopted on August 14, 2002. Among other things, the modifications addressed the following aspects of the Privacy Rule:
>
> - Uses and disclosures for treatment, payment and health care operations, including eliminating the requirement for the individual's consent for these activities;
> - The notice of privacy practices that covered entities must provide to patients (and adding "acknowledgment form");
> - Uses and disclosures for marketing purposes;
> - Minimum necessary uses and disclosures;
> - Parents as personal representatives of un-emancipated minors;
> - Uses and disclosures for research purposes; and
> - Transition provisions, including business associate contracts.

(OCR HIPAA privacy guidance, December 3, 2002, pate 7-8). [HHS has prepared a "fact sheet" relating to final modifications of the privacy rule. This fact sheet can be accessed on the World Wide Web at http://www.hhs.gov/news/press/2002pres/20020809.html]

Pages 3 - 7 highlight the August 2002 modifications. Pages 8 - 9 provide a comparison from December 2000 to the August 2002 modifications.

Starting on page 10 is the overview of the August 2002 modifications.

SUMMARY OF AUGUST 2002 MODIFICATIONS TO FINAL HIPAA PRIVACY RULE

1. 45 CFR 164.501: Employment Records.

   The definition of "protected health information" (PHI) now excludes "employment records held by a covered entity in its role as employer." Thus, employment records are not subject to the privacy rule. The United States Department of Health and Human Services does not define within the privacy rule itself "employment records held by a covered entity in its role as employer." HHS does, however, provide several examples in the August 2002 preamble including examples such as records for compliance with the Family Medical Leave Act (FMLA) or the Americans with Disabilities Act (ADA), drug tests and fitness for duty tests.

   If a covered entity provides health care to an employee the results of that health care will be considered PHI. The same information, however, will not be considered PHI when the information becomes part of the employment record. If a nurse in a hospital is administering a drug test to a fellow employee, the nurse must protect the results of that test consistent with the HIPAA privacy rule. If the employee also signs an authorization permitting the human resources department of the hospital to use the results for employment purposes, the results once they are transferred or a copy is made and the same information is placed in the hands of the human resources department, the "human resource record" will not be considered PHI subject to the privacy rule. The hospital record will still be protected by HIPAA. This is very similar to the statement on a 45 CFR 164.508 authorization form indicating that once information is disclosed to an individual or an entity not subject to the privacy rule, the information could be re-published or re-disclosed.

2. 45 CFR 164.501 and 45 CFR 164.508(a)(3): Marketing.

   The rule modifies the definition and requires an authorization to use and disclose PHI for marketing with limited exceptions.

3. 45 CFR 164.502(a)(1)(iii): Incidental Uses and Disclosures.

   A covered entity will not be found in violation of the HIPAA privacy rule if PHI is used or disclosed incident to a permitted use or disclosure as long as:

   1) Reasonable and appropriate safeguards are in place; and

   2) The entity complies with the minimum necessary requirement.

   A covered entity will not be in violation of the HIPAA privacy rule for uses or disclosures that are "byproducts" of acceptable uses and disclosures. A provider may instruct an administrative staff member to bill a patient for a particular procedure and may be overheard by one or more persons in the waiting room. If the provider has made reasonable efforts to avoid being overheard and reasonably

limited the information shared, then the incidental disclosure resulting from such conversation is permissible under the rule. Additionally, incidental disclosures are not required to be included in the accounting of disclosures found at 45 CFR 164.528.

4. 45 CFR 164.502(g)(3): Un-emancipated Minors.

The general rule and exceptions relating to un-emancipated minors remains unchanged after the final August 2002 modifications. HHS did revisit this issue and re-emphasized its position in yielding to state law. The general rule is that where applicable law gives a parent, a guardian, or person acting in loco parentis, the authority to make health care decisions on behalf of an un-emancipated minor, a covered entity must treat the parent, guardian, or person acting in loco parentis as a personal representative for purpose of the HIPAA privacy rule.

HIPAA does recognize that under certain circumstances the parent, guardian or person acting in loco parentis may not be treated as a personal representative, and the minor must be treated as an individual for purposes of the privacy rule:

- If the minor consents to the health care service and no other consent is required by law unless the minor requests the parent, guardian or person acting in loco parentis be treated as the personal representative.

- If the minor may lawfully obtain care without the consent of a parent, guardian or person acting in loco parentis, and the minor, a court, or another person authorized by law consents to the service, the parent, guardian, or person acting in loco parentis may not be treated as the personal representative.

- If the minor's parent, guardian, or person acting in loco parentis assents to an agreement of confidentiality between a health care provider and the minor regarding a health care service, then the minor's parent, guardian or person acting in loco parentis may not be treated as the minor's personal representative with respect to PHI pertaining to that service.

(These 3 exceptions are subject, however, to the "final modifications" that appear immediately below.)

The final modifications clarify the provisions requiring deference to state or other law in certain circumstances. These are summarized below:

- If state or other law permits or requires a covered entity to disclose or provide access to PHI about an un-emancipated minor to a parent, guardian or person acting in loco parentis, a covered entity may disclose or provide access to PHI to the extent permitted or required by that other law.

- If state or other law prohibits a covered entity from disclosing or providing access to PHI about an un-emancipated minor to a parent, guardian or person acting in loco parentis, a covered entity may not disclose or provide access to PHI to the extent prohibited by that other law.

- If the parent, guardian or person acting in loco parentis is not the un-emancipated minor's personal representative and there is no applicable law or other law relating to access by a parent, guardian or person acting in loco parentis, a covered entity may provide or deny access to a parent, guardian or person acting in loco parentis. The covered entity's decision to provide or deny access must be made by a licensed health care professional who in the exercise of professional judgment has made a determination in this area and it must be consistent with state or other applicable law.

5. 45 CFR 164.504: Hybrid Entity Definition.

A covered entity may designate itself as a hybrid entity if:

1) The entity is a single legal entity;

2) The entity's business activities include both covered and non-covered functions; and

3) The entity designates health care components.

If a covered entity designates itself a hybrid entity, its health care components:

1) Must include any component that would be a covered entity if it were a free-standing entity;

2) May include other components only to the extent that they perform covered functions;

3) May include other components only to the extent that they perform activities that would make the component a business associate of the health care component if the two components were separate legal entities.

6. 45 CFR 164.506: Treatment, Payment and Health Care Operations.

HIPAA privacy consent is not required for using or disclosing PHI for treatment, payment and health care operations (TPO). A covered entity is permitted to obtain consent for TPO but as of August 2002 such consent is now optional.

Without consent, a covered entity may:

1) Use or disclose PHI for its own TPO;

2) Disclose PHI for treatment activities of a health care provider;

3) Disclose PHI to another covered entity or health care provider for the payment activities of the recipient;

4) Disclose PHI to another covered entity for health care operation activities of the recipient if:

   a) Each entity either has or had a relationship with the individual; and

   b) The PHI pertains to that relationship; and

   c) The disclosure is for only limited types of health care operation activities as specified in the modified rule.

7. 45 CFR 164.508: Authorizations.

The revised final HIPAA privacy rule specifies only one type of authorization form where the original privacy rule included several types of authorization forms.

Disclosures made pursuant to an authorization are not required to be included in the accounting of disclosures requirements found in 45 CFR 164.528.

The single authorization form must include required “core elements” and “required statements.”

8. 45 CFR 164.512(i): Research.

The rule makes several significant changes to provisions relating to research.

9. 45 CFR 164.514(e): Limited Data Sets.

The final modifications to the HIPAA privacy rules establish an entirely new type of permitted use or disclosure. A covered entity is permitted to use or disclose a "limited data set" for public health, research or health care operation purposes if the entity enters into a "data use agreement" with the recipient of the data set.

The limited data set requires the removal of a specific list of individual identifiers. This list is shorter than the list required to make the information de-identified. The regulation specifies many of the items that must be included in a data use agreement. The data use agreement is similar in scope to a business associate agreement in that it requires the recipient to take certain steps to protect the PHI.

10. 45 CFR 164.520(c)(2)(i): Notice of Privacy Practices.

A health care provider that has a direct treatment relationship with an individual must make a good faith effort to obtain a written acknowledgment from the individual that he or she received the provider's notice of privacy practices. If the provider fails to obtain the acknowledgment for whatever reason, it must document its good faith effort and the reason why it did not obtain the acknowledgment.

A provider is not required to make a good faith effort to obtain an acknowledgment in an emergency treatment situation but after the emergency passes must then make the good faith effort to obtain such acknowledgment.

11. 45 CFR 164.528(b)(4): Accounting of Disclosures.

The modified HIPAA privacy rule includes several changes to the requirements for accounting of disclosures, including providing for an alternative procedure applicable in certain research related situations. Disclosure of information pursuant to a valid written authorization does not have to be reported on the accounting log. Disclosures for public health purposes and other matters under 45 CFR 164.512 must be recorded on the accounting log unless temporarily suspended pursuant to this section.

SUMMARY OF SELECTED MODIFICATIONS TO HIPAA PRIVACY RULE (August 2002)	
December 2000	**August 2002**
CONSENT: -- Direct treatment providers must obtain written consent for TPO except in limited circumstances.	-- Written Consent would be ***optional***. -- Replaced with requirement for written "acknowledgment" of receipt of *Notice of Privacy Practices.* -- Must make "good faith effort" to get acknowledgment signed - must record efforts if acknowledgment form not signed. If acknowledgment not obtained then the regulation would permit the use or disclosure for TPO.
DISCLOSURES FOR TPO OF ANOTHER CE: -- CEs can disclose PHI for treatment. -- CEs cannot disclose PHI for payment purposes of other CEs.	– Can use or disclose PHI for its own purposes without prior consent or authorization. -- Can also share PHI for treatment activities of another health care provider. -- Would permit disclosure of PHI for the payment activities of another CE (no authorization would be required) -- Could share PHI with another CE for the payment activities of that other CE. -- Could disclose PHI to another CE for certain listed health care operations of the other CE. (Requires each CE to have/had relationship with the patient.)
NOTICE OF PRIVACY PRACTICES -- Must present NPP with Consent at first time service is delivered after the compliance date. (Need to obtain written consent & provide NPP and give NPP to patient if asked for)	-- Direct treatment provider must make a good faith effort to obtain written "acknowledgment" from patient of receipt of the CE's NPP. – Has exception for emergency treatment but must use efforts to obtain "acknowledgment" after the emergency passes. -- Must be done at "first service time is delivered." -- Must give copy of NPP to each patient at first service delivery time on or after April 14, 2003. -- Can use mailing method (mail NPP to patients with "tear off" acknowledgment form to be signed and returned).

MINIMUM NECESSARY & ORAL COMMUNICATIONS:	-- Permits incidental uses & disclosures - mostly oral communications. Must have reasonable safeguards in place. Minimum necessary would not apply to an authorization received from a patient.
BUSINESS ASSOCIATES:	-- Provides sample BAC language. -- Extends times for BAC to one year pass April 14, 2003..... but only as to existing contracts that are in place before October 2002 and otherwise modified.
MARKETING: -- Permits "marketing" if you give the individual the opportunity to "opt-out" of future marketing.	-- Eliminates the "opt-out" provision. All "Marketing" would require an "authorization." "Marketing" is defined and excludes a CE's participation in a health care provide network or health plan network, or to describe if, and the extent to which, a product or service is provided by a CE or included in a plan of benefits, treatment of that individual, or case management or care coordination or to direct/ recommend alternative treatments, therapists, health care providers, or settings of care, and "face-to-face" communications made by a CE to an individual. Clarifies "nominal value" to mean "promotional gift of nominal value."
MINORS:	-- Will continue to defer to state or other applicable law and to remain neutral and preserve the status quo to the extent possible.
AUTHORIZATIONS: -- Requires at least 3 authorizations depending on the purpose.	-- Combines all authorizations into one authorization form with required core elements and "required statements".
DE-IDENTIFICATION OF PHI	-- Removes de-identification code or other means of record identification from listed identifiers.
ACCOUNTING:	-- Disclosures made under a patient's authorization not required to be included in the accounting log.
HYBRID ENTITIES -- The "covered function" could not be the "primary function" of the CE.	-- The "covered function" of a single legal entity could be the "primary function" of the CE.
PROTECTED HEALTH INFORMATION:	-- "Expressly" excludes employment records from definition of PHI.

1. GENERAL RULE: WHO AND WHAT ARE COVERED

General Rule: The final privacy rule establishes a general rule as follows:

> "A ***covered entity*** [CE] may not use or disclose an individual's ***protected health information*** [PHI] , except as otherwise permitted or required by this subpart." 45 CFR 164.502(a).

[A **CE** is defined on page 11. **PHI** is defined on page 20.]

This analysis relates to modifications made in the HIPAA privacy rule in August 2002. (67 Fed. Reg. 53182). This analysis relates only to the HIPAA privacy rule and does not provide a "preemption" analysis under Kansas law. Built into the HIPAA privacy rule, however, is a federal floor relating to privacy of health information.

Preemption Overview: Section 1178 of the Social Security Act gave the Secretary of Health and Human Services powers to impose preemption on narrow grounds. Under 45 CFR 160.203 the general rule is established that a "standard requirement, or implementation specification adopted under this [HIPAA privacy] subchapter that is contrary to a provision of state law preempts the provision of state law." It is then further stated that this general rule applies except in certain circumstances. One such circumstance is when the determination is made by the Secretary of HHS in four specific circumstances or a state law that has as its principal purpose the regulation of the manufacturer, registration, distribution, dispensing, or other control of any controlled substances or that is deemed a controlled substance by state law. See 45 CFR 160.203.

Additionally, 45 CFR 160.203(c) exempts state laws or procedures that pertain to reporting of certain diseases or public health surveillance. Section 45 CFR 160.203(d) exempts state health plan requirements for access to certain financial and management controls for program monitoring and licensure. In August 2002, HHS reinforced its commitment that its deference to state laws regarding health information of minors will be controlling. See 45 CFR 164.502(g)(3)(ii)(A), (B), and (C) and 67 Fed. Reg. 53200.

2. THE APPLICATION OF THE GENERAL RULE AS IT RELATES TO THE DEFINITION OF "COVERED ENTITY" AND "PROTECTED HEALTH INFORMATION"

Definitions: **COVERED ENTITIES:** The final rule defines covered entities to include:
health plans,
health care providers and
health care clearinghouses (which for the most part relate to public or private billing services). 45 CFR 160.103.

Each of the following is a "***covered entity***" as defined under the final rule:

- A covered "***health care provider***"[1] is a health care provider who transmits any health information[2] in electronic form in connection with a standard transaction.[3] For purposes of the final rule, health care providers generally include providers of medical or health services and other persons or organizations that furnish, bill, or are paid for health care in the normal course of business. 45 CFR 160.103.

[1] Health care provider: means a provider of services (as defined in Section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in Section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills or is paid for health care in the normal course of business.

[2] Health information: means any information whether oral or recorded in any form or medium that:
(1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
(2) relates to the past, present or future physical or mental care to an individual; or past, present or future payment for the provisions of health care to an individual.

[3] Transaction: means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:
1. Health care claims or equivalent encounter information,
2. Health care payments and remittent advice,
3. Coordination of benefits,

4. Health care claim status,
5. Enrollment and disenrollment in a health plan,
6. Eligibility for a health plan,
7. Health plan premium payments,
8. Referral, certification and authorization,
9. First report of injury,
10. Health claims attachments,
11. Other transactions that the secretary may prescribe by regulation.

- A covered "***health plan***" is generally an individual or group plan, whether private or governmental, that provides or pays the cost of medical care. Covered health plans include, but are not limited to, health insurance insurers [defined as any insurance company licensed and regulated by a state], insurers of a long-term care or Medicare supplemental policies, HMOs, ERISA plans providing medical care, and most government health care programs [Medicare, Medicaid, active duty military, Tri-Care, etc.].

- A covered "***health care clearinghouse***" is any public or private entity that converts health information it receives in a non-standard form into a standard health information form or transaction, that is referred to as a "standard transaction", or that converts a standard transaction that it receives into a non-standard form for another entity. Health care clearinghouses may include billing services, re-pricing companies, community health information systems, and "value added" networks and switches. 45 CFR 160.103.

CMS Website for Assistance: The Center for Medicare and Medicaid Services (CMS) provides a decision making tool at its website to help determine if you are a covered entity:

http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

3. SPECIAL TYPES OF COVERED ENTITIES:

Definitions: A "***covered entity***" (CE) may enter into an arrangement with another covered entity and, thus, be considered an "***affiliated***" entity or fall under the definition of a "***hybrid***" entity. CEs may also enter into organized health care arrangements. Special conditions must be met. These special types of covered entities are addressed below.

HYBRID AND AFFILIATED COVERED ENTITIES:

Covered entities may enter into arrangements with other covered entities to assist with compliance with regulatory requirements. Some covered entities that do not have as their primary focus the delivery of health care but do provide heath care on some level are also given a special title. These special groups are explained below:

- A "***hybrid entity***" means a single legal entity that is a CE whose business activities include both covered and non-covered functions and that designates health care components of it to include any component that would meet the definition of a CE if it were a separate legal entity. Additionally, health care components may include a component that performs covered functions and activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities. This permits a ***"hybrid entity"*** to designate otherwise non-covered functions or portions of its operations that provide service to the covered functions, such as parts of a legal or accounting divisions of the entity, as part of the health care component, so that PHI could be shared with such functions of the entity without business associate agreements or individual authorizations.

  August 2002 modification reference"hybrid entity": HHS has eliminated the word "primary" from the definition of ***"hybrid entity"*** as it appeared in 45 CFR 164.504(a) in December 2000. Now, any covered entity that otherwise qualifies and that designates health care components in accordance with 45 CFR 164.504(c)(3)(iii) is a ***"hybrid entity.***" 67 Fed. Reg. 53205. HHS stated in August 2002 that a CE is still subject to minimum necessary restrictions under 45 CFR 164.502 and 45 CFR 164.514(d), and, thus, must have policies and procedures that describe who within the entity may have access to the PHI. Under these provisions, according to HHS, workforce members may be permitted access to PHI only as necessary to carry out their duties with respect to the entity's covered functions .67 Fed. Reg. 53205

  An "***affiliated covered entity***" consists of legally separate covered entities which are affiliated under common ownership (defined as 5% or more ownership or equity interest) or common control (defined to include both direct or indirect power to significantly influence actions and policies), and which designate themselves as a single entity for purposes of compliance with the final privacy rules. An example is a corporate hospital chain may

designate all of its hospitals as one affiliated covered entity. As with hybrid entities, affiliated covered entities must segregate protected information within their joint information system to regulate the use and disclosure between their various covered and non-covered functions. This type of entity can use a "single shared notice of information practices and a consent form." 65 Fed. Reg. 82503. 45 CFR 164.504 and 65 Fed. Reg. at 82503.

A ***"multiple function" covered entity*** occurs when a covered entity performs multiple covered functions that would make the entity any combination of a health plan, health care clearinghouse, or health care provider. In such a case, the entity must comply with the final privacy rules only to the extent applicable to each covered function. Multiple covered function entities may include certain integrated health plans or health care delivery systems that act as both health plans and health care providers. The same segregation requirements that are applicable to an affiliated covered entity and a hybrid entity apply to multiple function covered entities. 45 CFR 164.504 and 65 Fed. Reg. at 82503.

ORGANIZED HEALTH CARE ARRANGEMENT:

Special issues exist for health systems and medical groups that desire or have the appearance that they operate as one. The final privacy rule creates a new type of covered arrangement that accommodates these integrated entities that consist of more than one covered entity. This type of arrangement is called an "***organized health care arrangement***." This "organized health care arrangement" includes:

- clinically integrated care settings in which an individual receives care from more than one provider (the basic example is a group physician practice and hospitals where the physicians have privileges and provide care);

- organized systems of health care including more than one covered entity holding itself out to the public as a joint arrangement and participating in joint activities;

- a group health plan and one or more health insurance insurers are HMOs; two or more group health plans maintained by the same plan sponsor; and

- two or more group health plans maintained by the same plan sponsor in health insurance insurers or HMOs. An example is a manufacturing company that has an on-site industrial health clinic. The clinic and the administrative and business functions performed by the company with respect to the clinic would be required to comply with the final privacy rules as a covered entity. 45 CFR 164.501.

August 2002 modification reference OHCAs: In August 2002, HHS clarified that with the modification to 45 CFR 164.506(c)(5), covered entities that participate in an OHCA may share PHI for the health care operations of the OHCA, without the condition that each covered entity have a relationship with the individual who is the subject of the information.

The final modified privacy rule requires that joint notice of an OHCA to reflect the fact the notice covers more than one CE and that, if applicable, the CEs participating in an OHCA will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations (TPO) relating to the OHCA. This is specifically addressed at 45 CFR 164.520(d).

Commentary: Questions have arisen as to the suitability and feasibility of an organized health care arrangement after the August 14, 2002 modifications to the final privacy rule. In August 2002, HHS provided regulatory authority for health care providers to share PHI across the treatment continuum with other health care providers whether they are covered entities or not. Additionally, in August 2002, HHS, again by regulatory authority, has permitted covered entities to disclose PHI for payment purposes of the requesting health care provider. Further, HHS has provided, through its regulatory authority enacted in August 2002, that health care providers/covered entities may disclose PHI for selected health care operations of other CEs. With this regulatory authority and the elimination of the mandatory consent requirement, the advantages of an OHCA are somewhat diminished. One commentator, HCPro, Executive Briefings Digest, December 17, 2002, Vol. 3, No. 50, has identified "pros and cons" of an OHCA. According to HCPro, the "appeal of an OHCA lies mainly with the ability to do the following:

- Use one notice of privacy practices for all participants.
- Enable sharing of PHI between participants for purposes of their integrated operations.
- Spread out the investment in privacy compliance across the greatest possible spectrum of stakeholders."

The "cons" associated with forming an OHCA under the HCPro briefing is as follows:

- "Uncertainty over requirements for documenting or showing evidence of the existence of the OHCA.
- Risk of shared liability for shared undertakings.
- Ambiguity about the boundaries and the relationships between an OHCA and its component covered entity providers."

The risk for shared liability has not been addressed from a regulatory or statutory standpoint and is a major issue to be resolved by all health care providers prior to entering into an OHCA. Additionally, while one of the "pros" identified by the Briefings is the spreading out of the investment, such much be weighed against state and federal anti-kickback issues associated with the providing of a service or an item of value to include the providing of a salaried privacy officer paid for by a hospital but providing services to and functioning as a privacy officer for any physician practice group in an OHCA arrangement with the hospital.

4. BUSINESS ASSOCIATES OF COVERED ENTITIES:

Background and Definition: A "business associate" of a covered entity is also affected by the final rules. The compliance requirements with respect to a business entity are somewhat different than the rules applicable to a "covered entity" itself. A business associate is a person or entity that (1) ***performs certain activities on behalf of, or*** (2) ***provides certain services to***, a covered entity or an "organized health care arrangement" in which the covered entity participates (which activity or services includes the use or disclosure of protected health information).

A CE may be a business associate of another CE, but a business associate of a covered entity participating in an organized health care arrangement does not automatically become a business associate of other covered entities participating in the arrangement. This means that if a covered entity has a business associate relationship through a business associate contract and the covered entity then participates in the organized health care arrangement the business associate does not become a business associate of the other participants.

A CE must have a "Business Associate Contract" (BAC) in place with the Business Associate (BA) ***before*** the BA does any work for the CE that involves the receipt of PHI. HHS has provided in the August 14, 2002 *Federal Register* sample language for a BAC.

http://www.hhs.gov/ocr/hipaa/contractprov.html

This sample BAC will need additional elements to make it a binding contract under applicable law.

August 2002 modifications reference Business Associates: In August 2002, HIPAA privacy rule transition provisions of 45 CFR 164.532(d) and (e) were modified to permit covered entities, other than small health plans, to continue to operate under certain existing contracts with business associates for up to one year beyond April 14, 2003. This transition period is available to covered entities who have an existing contract with a business associate prior to the effective date of the privacy rule modification, provided that the contract is not renewed or modified prior to April 14, 2003. CEs with contracts that qualify are permitted to continue to operate under those contracts with their BAs until April 14, 2004, or until the contract is renewed or modified, whichever is sooner. 67 Fed. Reg. 53249.

Decision Trees / Charts: Two decision trees are included here for your review. The first "tree" is a "Business Associate General Rule Decision Chart." It assists a reader to determine if a person or entity is a business associate. The second decision "tree" assists a reader in determining if a business associate contract (BAC) is needed or not, depending upon what the receiving person or receiving entity's use of the PHI would be. These are on pages 57 and 58.

BA List: Business associate functions and activities include claims processing or administration; data analysis, process or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate "services" are identified as legal, actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. See definition of business associate at 45 CFR 160.103. Also see OCR HIPAA privacy guidance, December 3, 2002, page 40.

OCR Examples of non-BAs: Examples provided by OCR in which a business associate contract "or other written agreement" is not required to be in place before PHI may be disclosed are as follows:

- Disclosures by a covered entity to a health care provider for treatment of the individual.

- A hospital is not required to have a business associate contract with a specialist to whom it refers a patient and transmits the patient's medical chart for treatment purposes.

- A physician is not required to have a business associate contract with a laboratory as a condition of disclosing PHI for the treatment of an individual.

- A hospital laboratory is not required to have a business associate contract to disclose PHI to a reference laboratory for treatment of the individual.

- When a health care provider discloses PHI to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. [The explanation provided by OCR is that a provider that submits a claim to a health plan and a health plan that accesses and pays the claim are each acting on its own behalf as a covered entity, and not as a "business associate" of the other.]

- With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all.

- With a person or organization that acts merely as a conduit for protected health information, for example, the U.S. Postal Service, certain private carriers, and their electronic equivalents.

- Among covered entities who participate in an organized health care arrangement to make disclosures that relate to the joint health care activities of the OHCA.

- When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, in initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health care premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.

OCR HIPAA privacy guidance, December 3, 2002, pages 42-43.

SPECIAL NOTE - Incidental Disclosures, BACs, and Confidentiality Agreements: OCR in clarifying that "janitorial services" do not require a business associate contract indicates that any disclosure of PHI is limited in nature, occurs as a byproduct of the janitorial duties, and could not be reasonably prevented. Accordingly, such disclosures are incidental and permitted by the HIPAA privacy rule under 45 CFR 164.502(a)(1). OCR takes a different position, however, if a service is hired to do work for a covered entity where disclosure of PHI is not limited in nature and OCR describes such as routine handling of records or shredding of documents containing PHI OCR states that it is "likely" such would be considered a business associate. However, according to OCR, when such work is performed under the direct control of the covered entity on the covered entity's premises, the privacy rule permits the covered entity to treat the service as part of its work force, and the covered entity need not enter into a business associate contract with the service. OCR HIPAA privacy guidance, December 3, 2002, page 48. Even if a business associate contract is not necessary for these types of services it is recommended that at a minimum a confidentiality agreement be entered into prohibiting the re-publication, re-release or disclosure of any PHI. An example where a special service would require a business associate contract is a software company that hosts the software containing patient information on its own server or access patient information when trouble-shooting software functions. OCR privacy guidance, December 3, 2002, page 53.

5. WHAT IS PROTECTED?

PROTECTED HEALTH INFORMATION:

Background: In the final privacy rules ***protected health information***, commonly referred to as "PHI", includes information transmitted or maintained in any form or medium, including oral communications.

PHI does not include, however, health information contained in certain education records, student medical records and employment records maintained by a covered entity in its capacity as an employer. 45 CFR 164.501.

SPECIAL NOTE: August 2002 clarification reference health care facility as the *employer*: The medical record of a hospital employee who is receiving treatment at the hospital is PHI and is covered by the privacy rule, just as the medical record of any other patient of that hospital. The hospital may use that PHI only as permitted by the privacy rule, and in most cases will need the employee's authorization to access or use the medical information for employment purposes (a non-TPO purpose). When the individual gives his or her medical information to the CE as the employer, such as when submitting a doctor's statement to document sick leave, or when the CE as the employer obtains the employee's written authorization for disclosure of PHI, such as an authorization to disclose the results of a fitness-for-duty examination, the medical information becomes part of the employment record, and, as such, is no longer PHI. Additional employment records as identified by HHS include files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees may be maintained as part of the CE's employment records. 67 Fed. Reg. 53192

Health information in any form is protected (and called *Individually Identifiable Health Information*) if it:

1. Is created or received by a covered entity;

2. Relates to an individual's past, present, or future physical or mental health condition, the provision of health care to an individual or the payment for the provision of health care to an individual; **and**

3. Identifies the individual or creates a reasonable basis to believe that the information, including demographic information, may be used to identify the individual. 45 CFR 160.103 (Moved from 45 CFR 164.501 in August 2002).

"Health information" would include records in possession of a health care provider that are from other providers.

The term "health information" is broadly defined under the final rules and for the most part will relate to any care or service - past, present or future - provided to an individual and also relates to payment for the provision of health care to an individual. This information is limited to the health information that is created or received by a covered entity for certain other entities. 45 CFR 160.103.

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION:
"Individually identifiable health information" is a subset of health information, including demographic information, that identifies the individual or can be used to identify the individual. 45 CFR160.103. The complete definition is found at 67 Fed. Reg. 53266.

DE-IDENTIFIED HEALTH INFORMATION:
A covered entity may use PHI to create de-identified health information by removing 18 identifiers such as names, addresses, dates, photographs, and various identification numbers. The de-identified information would then be in such a form that does not identify an individual and is with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Once health information is de-identified, it is not longer protected or covered by the final rules. De-identified health information must be created in accordance with the procedures outlined in 45 CFR 164.514(a). See 45 CFR164.502 and 514. The re-identification code or other means of record identification permitted by 45 CFR 164.514(c) is expressly excepted from the listed safe harbor identifiers found at 45 CFR 164.514(b)(2)(i)(R). 67 Fed. Reg. 53233.

August 2002 modification creates new limited data set: The August 2002 modifications permit use of certain information that is called a "limited data set." Accordingly to some this "limited data set" is more useful data but its use is restricted to research, public health, and health care operations. "Limited data sets" require a "data use agreement which limit the uses and access to the data sets and require that the recipients do not attempt to re-identify the patients. The following table compares the "de-identification" factors that must be removed so that the information is no longer considered PHI and the direct identifiers that are removed to create a "limited data set."

Comparison between "de-identification identifiers" and "Limited Data Set" direct identifiers	
De-identification identifiers under 45 CFR 164.514	**Direct identifiers under a Limited Data Set**
Names	Names
All geographic subdivisions small than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if certain conditions are met,	Postal address information, other than town or city, State, and zip code
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 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.	
Telephone numbers	Telephone numbers
Fax numbers	Fax numbers
Electronic mail addresses	Electronic mail addresses
Social security numbers	Social security numbers
Medical record numbers	Medical record numbers
Health plan beneficiary numbers	Health plan beneficiary numbers
Account numbers	Account numbers
Certificate / license numbers	Certificate / license numbers
Vehicle identifiers and serial numbers, including license plate numbers	Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers	Device identifiers and serial numbers
Web Universal Resource Locators (URLs)	Web Universal Resource Locators (URLs)
Internet Protocol (IP) address numbers	Internet Protocol (IP) address numbers
Biometric identifiers, including finger and voice prints	Biometric identifiers, including finger and voice prints
Full face photographic images and any comparable images	Full face photographic images and any comparable images
And other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of 45 CFR 164.514.	

6. WHAT CAN BE RELEASED, WHEN, AND TO WHOM?

GENERAL PRIVACY AND ACCESS REQUIREMENTS: Compliance with the final privacy rules will require observance of complex privacy and access requirements for PHI. The general rule imposed is that protected health information may not be used or disclosed by the covered entity except as specifically detailed in the final rules. 45 CFR 164.502. The final privacy rules also create a new set of rights for patients with respect to PHI requiring the covered entities to provide patients with benefits such as notice of privacy practices, access to health information in certain circumstances, and accounting of health information disclosures in certain circumstances. 45 CFR 164.502.

LIMITATIONS ON USE AND DISCLOSURE: A covered entity is generally permitted to use or disclose protected health information only (includes August 2002 modifications):

(1) To the individual patient (or to the individual patient's personal representative, as applicable);

According to OCR under the privacy rule a person authorized (under state or other applicable law, e.g., tribal or military law) to act on behalf of the individual in making health care related decisions is the individual's "personal representative." OCR HIPAA privacy guidance, December 3, 2002, page 29. OCR continues that "in general," the scope of the personal representative's authority to act for the individual under the privacy rule derives from his or her authority under applicable law to make health care decisions for the individual. Accordingly, OCR states that when a person has broad authority to act on behalf of a living individual in making decisions relating to health care, such as a parent with respect to a minor child or a legal guardian of a mentally incompetent adult, the covered entity must treat the personal representative as the individual for all purposes under the rule, unless an exception applies such as with respect to abuse, neglect or endangerment situations and in the application of state law in the context of parents and minors. Where the authority to act for the individual is limited or specific to particular health care decisions, OCR's position is the personal representative is to be treated as the individual only with respect to PHI that is relevant to the representation. OCR HIPAA privacy guidance, December 3, 2002, page 30. OCR states that the covered entity should not treat that person with the limited authority as the individual for other purposes, such as to sign an authorization for the disclosure of PHI for marketing purposes. OCR HIPAA privacy guidance, December 3,

2002, page 30. OCR does state, however, that the HIPAA privacy rule does require covered entities to verify a personal representative's authority in accordance with 45 CFR 164.514(h).

(2) For treatment, payment, or health care operations, as permitted by and in compliance with 45 CFR 164.506 (regulatory authority to use PHI for TPO and optional consent provision);

(3) Incidental uses and disclosures of PHI. [In August 2002 HHS adopted a provision that explicitly permits certain incidental uses and disclosures that occur as a byproduct of a use or disclosure otherwise permitted under the privacy rule and incidental use or disclosure is permitted only to the extent that the covered entity has applied reasonable safeguards as required by 45 CFR 164.530(c), and implemented the minimum necessary standard, where applicable, as required by 45 CFR 164.502(b) and 45 CFR 164.514(d). HHS has stated that an incidental use or disclosure that occurs as a result of the failure to apply reasonable safeguards or the minimum necessary standard, where required, is not a permissible use or disclosure and, therefore, is a violation of the privacy rule. Additionally, incidental disclosures are not required to be recorded on the accounting of disclosures under 45 CFR 164.528. This new provision permits the use of sign-in sheets and calling out of names in waiting rooms so long as the information disclosed is appropriately limited. Additionally, disclosure of PHI in a group setting would be a treatment disclosure and thus permissible without individual authorization. HHS has taken the position that the reasonable safeguards and minimum necessary standards, addressed above, are flexible and adaptable to the specific business needs and circumstances of the CE. 67 Fed. Reg. 52193-94]

(4) Upon receipt of a proper and valid authorization;

(5) Upon a patient's agreement or failure to object following an opportunity to object in certain circumstances; and

(6) Under certain public policy provisions. 45 CFR 502, 506, 508, 510 and 512.

A covered entity is required to disclose PHI upon a request by the individual pursuant to the final rules (which does include certain restrictions mostly in the mental health arena) or when requested by Health and Human Services for purposes of investigation or determining compliance. 45 CFR 164.502.

7. MINIMUM NECESSARY USE OR DISCLOSURE:

General Rule: A covered entity must make reasonable effort to limit the use, disclosure of and request for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. 45 CFR 164.502(b).

The minimum necessary standard applies when a covered entity uses or discloses PHI or requests PHI from another covered entity.

Exceptions: This standard does not apply, however, to:

Disclosures to or requests by a health care provider for treatment;

1. Disclosures to or requests by a health care provider for treatment;

2. Uses or disclosures made to individuals about their own PHI;

3. Uses or disclosures made pursuant to an authorization;

4. Uses or disclosures made to the Secretary in accordance with the final rules;

5. Uses or disclosures that are required by law, as further described in 45 CFR 164.512(a);

6. Uses or disclosures that are required for compliance with applicable requirements of the privacy rule.

Requirements: Compliance with the minimum necessary requirement requires covered entities to limit health information, use and disclosure to necessary employees and necessary categories of information.

Compliance also requires implementation of policies and procedures to limit routine disclosures and requests to reasonably necessary information, and further requires the evaluation of non-routine disclosures and requests on an individual basis using established criteria. This provision relating to routine disclosures permits covered entities to avoid case-by-case determinations under the minimum necessary standard for routine and recurring requests for disclosures, such as completing claim forms.

A CE is required to develop and implement policies and procedures appropriate to the CE's business practices and work force that reasonably minimizes the amount of PHI used, disclosed and requested. For uses of PHI, the policies and procedures must identify the persons or classes of persons within the CE who need access to the information to carry out their job duties, the categories or types of protected health information needed, and the conditions appropriate to such access. For routine or recurring requests and

disclosures, the policies and procedures may be standard protocols. Non-routine requests for, and disclosures of, PHI must be reviewed individually. 45 CFR 164.514(d)

As between two covered entities, the requesting entity has the burden of limiting its requests to reasonably necessary information, allowing the disclosing entity to rely on the request as being appropriately limited. 45 CFR 164.502 and 514(d)(3)(iii).

August 2002 modification – Incidental Uses and Disclosures

HHS proposed to modify and did change the December 2000 privacy rule to add a new provision at 45 CFR 164.502(a)(1)(iii) which "explicitly" permits certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure under the privacy rule.

An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a byproduct of an otherwise permitted use or disclosure under the privacy rule. The Department requires that an incidental use or disclosure is permissible only to the extent that the CE has applied reasonable safeguards as required by 45 CFR 164.530(c), and implemented the minimum necessary standards, where applicable, as required by 45 CFR 164.502(b) and 45 CFR 164.514(d). 67 Fed. Reg. 2195-6.

According to the OCR HIPAA privacy guidance a covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. OCR HIPAA privacy guidance, December 3, 2002, page 11. See 45 CFR 164.530(c). Therefore, any policy that a covered entity adopts that identifies and puts in place appropriate administrative, technical, and physical safeguards must also implement the minimum necessary standard and the policy must include a limit on incidental uses or disclosures.

August 2002 modification to the Minimum Necessary Standard

HHS separated 45 CFR 164.502(b)(2)(ii) into two subparagraphs at 45 CFR 164.502(b)(2)(ii) and (iii) to eliminate confusion regarding the exception to the minimum necessary standard for uses or disclosures made pursuant to an authorization under 45 CFR 164.508 and those disclosures made to the individual.

Additionally, HHS eliminated special authorizations required under the December 2000 privacy rule at 45 CFR 164.508(d)(e) and (f).

HHS expanded the exception for authorizations to apply generally to any authorization executed pursuant to 45 CFR 164.508. Therefore, the change would exempt from the minimum necessary standard any uses or disclosures for which a CE has received an authorization that meets the requirements of 45 CFR 164.508.

HHS modified 45 CFR 164.514(d)(1) to delete the term "reasonably ensure" in response to concerns that the term connotes an absolute, strict standard.

With respect to requests not made on a routine and recurring basis, HHS has noted that it omitted from 45 CFR 164.514(d)(4) a requirement that a CE may implement the standard by developing criteria designed to limit its request for PHI to the minimum necessary to accomplish the intended purpose. Accordingly, HHS added such a provision to make the implementation specifications for applying the minimum necessary standard to request for PHI by a CE more consistent with the implementation specifications for disclosures.

The OCR HIPAA privacy guidance states that covered entities must implement reasonable minimum necessary policies and procedures that limit how much PHI is used, disclosed, and requested for certain purposes. OCR goes on to state that these minimum necessary policies and procedures also reasonably must limit who within the entity has access to PHI, and under what conditions, based on job responsibilities and the nature of the business. OCR HIPAA privacy guidance, December 3, 2002, page 12. OCR clarifies that the minimum necessary standard does not apply to disclosures, including oral disclosures, among health care providers for treatment purposes. OCR HIPAA privacy guidance, December 3, 2002, page 12.

OCR interprets the privacy rule that it permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. According to OCR such reliance must be reasonable under the particular circumstances of the request. OCR indicates that the reliance is permitted when the request is made by:

- A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the rule, such as for public health purposes under 45 CFR 164.512(b).

- Another covered entity.

- A professional who is a work force member of the covered entity or a business associate of the covered entity holding the information and who states that the information requested is the minimum necessary for the stated purpose.

- A researcher with appropriate documentation from an Institutional Review Board (IRB) or privacy board.

- The privacy rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

OCR HIPAA privacy guidance, December 3, 2002, page 22-23.

Under the frequently-asked question section of “minimum necessary” in the OCR HIPAA privacy guidance of December 3, 2002, OCR states that the privacy rule permits a

provider who is a covered entity to disclose a complete medical record **including portions that were created by another provider**, assuming the disclosure is for a purpose permitted by the privacy rule, such as treatment. OCR HIPAA privacy guidance, December 3, 2002, page 27.

8. USE OR DISCLOSURE REQUIRING PATIENT CONSENT:

Background: The December 2000 HIPAA privacy rule required covered providers to obtain an individual's written consent prior to using or disclosing PHI for these purposes. Under this December 2000 provision health care providers would not have been able to use or disclose PHI for TPO prior to their initial face-to-face contact with the patient, something which is routinely done today to provide patients with timely access to quality health care. This is a point recognized by HHS in August 2002. To rectify this problem, HHS proposed that health care providers with direct treatment relationships with individuals would no longer be required to obtain an individual's consent prior to using and disclosing PHI about him or her for TPO. In the August 2002 privacy rule publication, HHS adopted this view.

August 2002 modification reference HIPAA Consents for TPO: Consents are now *optional* under the HIPAA privacy rule.

The final August 2002 HIPAA privacy rule makes the obtaining of consent to use and disclose PHI for TPO optional on the part of all covered entities, including providers with direct treatment relationships. A health care provider that has a direct treatment relationship with an individual is not required by the HIPAA privacy rule to obtain an individual's consent prior to using and disclosing information about him or her for TPO. These health care providers, like all other covered entities, now have regulatory permission for such uses and disclosures. 67 Fed. Reg. 53209.

Under the new regulatory authority provision to use PHI for TPO the emergency care, substantial communication and other exceptions found in the December 2000 privacy rule have been eliminated. Additionally, there is no longer mandatory elements for the optional consent form. It is recommended, however, should a covered entity desire to continue to use the now optional consent form that it craft the consent form based on the requirements present in the December 2000 HIPAA privacy rule that have now been eliminated as consent is now optional.

Even with making the consent optional any uses or disclosures of PHI for TPO must still be consistent with the CE's notice of privacy practice. It is important to note the removal of a consent requirement applies only to consent for TPO. It does not alter the requirement to obtain an authorization under 45 CFR 164.508 for uses and disclosures of PHI not otherwise permitted by the privacy rule or any other requirements for the use or disclosure of PHI.

In making the modification for consents under 45 CFR 164.506 HHS in its August 2002 preamble indicated it intends to enforce strictly the requirements for obtaining an individual's authorization, in accordance with 45 CFR164.508, for uses and disclosures of PHI for purposes not otherwise permitted or required by the HIPAA privacy rule. It is HHS' position that a consent obtained voluntarily would not be sufficient to permit a use or disclosure which, under the privacy rule, requires an authorization or is otherwise

expressly conditioned under the rule. For example, according to HHS, a consent under 45 CFR 164.506 could not be obtained in lieu of an authorization required by 45 CFR164.508.

Under the HIPAA privacy rule as modified in August 2002, a patient who disagrees with the CE's information practices as stated in the CE's notice of privacy practices, can choose not to receive treatment from that provider, or can obtain treatment despite concerns about the information practices. The patient can request, according to HHS, that the provider restrict the use or disclosure of the information. Additionally, the August 2002 change to the consent provision does not affect the right of an individual under 45 CFR 164.522(a) to request restrictions to a use or disclosure of PHI.

One of the most important provisions that has been clarified is that health care providers will not need a patient's consent to consult with other providers about the treatment of a patient. If, however, a health care provider is disclosing PHI to another provider for purposes other than TPO an authorization may be required under 45 CFR 164.508 according to HHS.

Permitted Uses of PHI: The HIPAA privacy rule at 45 CFR 164.506(c) was changed to permit the following:

1. States that a CE may use or disclose PHI for *its own* TPO.

   OCR in its HIPAA privacy guidance provided examples as follows:

   - A hospital may use PHI about an individual to provide health care to the individual and may consult with other health care providers about the individual's treatment.

   - A health care provider may disclose PHI about the individual as part of claim for payment to a health plan.

   - The health plan may use PHI to provide customer service to its enrollees. (OCR HIPAA privacy guidance, December 3, 2002, page 56.)

2. Clarifies that the CE may use or disclose PHI for the treatment activities of any health care provider.

   OCR in its HIPAA privacy guidance provided examples as follows:

   - A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.

- A hospital may send a patient's health care instructions to a nursing home to which the patient is transferred. (OCR HIPAA privacy guidance, December 3, 2002, page 56.)

3. Permits the CE to disclose PHI to another CE or any health care provider for the payment activities of the entity that receives the information.

   OCR in its HIPAA privacy guidance provided examples as follows:

   - A physician may send an individual's health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.

   - A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment and services. (OCR HIPAA privacy guidance, December 3, 2002, page 56.)

4. Permits a CE to disclose PHI to another CE for the health care operation activities of the entity that receives the information, ***if*** each entity either has or had a relationship with the individual who is the subject of the information, the PHI information pertains to such relationship and the disclosure is for one of the purposes listed in paragraphs (1) or (2) of the definition of "health care operations" which includes quality assessment and improvement activities; population-based activities relating to improving health or reducing health care costs, case management and care coordination; conducting training programs, and accreditation, licensing, or credentialing activities; or for the purpose of health care fraud and abuse detection or compliance.

   OCR in its HIPAA privacy guidance provided examples as follows:

   - A health care provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, provided that the health plan has or had a relationship with the individual who is the subject of the information.
     (OCR HIPAA privacy guidance, December 3, 2002, page 57.)

5. Clarifies that a CE that participates in an organized health care arrangement (OHCA) may disclose PHI about an individual to another entity that participates in the OHCA for any health care operation activities of the OHCA. According to HHS, CEs that participate in an OHCA may share PHI for the health care operations of the OHCA, without the condition that each CE have a relationship with the individual who is the subject of the information. (The privacy rule requires the joint notice of an OHCA to reflect the fact that the notice covers more

than one CE and that, if applicable, the CEs participating in the OHCA will share PHI with each other, as necessary to carry out TPO relating to the OHCA.) 67 Fed. Reg. 53216.

OCR in its HIPAA privacy guidance provided examples as follows:

- The physicians with staff privileges at a hospital may participate in the hospital's training of medical students. (OCR HIPAA privacy guidance, December 3, 2002, page 57.)

SPECIAL NOTE REGARDING USE AND DISCLOSURES OF *PSYCHOTHERAPY NOTES*. OCR notes that except when psychotherapy notes are used by the *originator* of the psychotherapy notes to carry out treatment, or by the covered entity for certain other limited health care operations, uses and disclosures of psychotherapy notes for treatment, payment, and health care operations require the individual's authorization. OCR HIPAA privacy guidance, December 3, 2002, page 57 citing to 45 CFR 164.508(a)(2).

Consent Form Contents Eliminated: If a CE decides to use the now optional consent form the requirements for the consent form set forth in the December 2000 HIPAA privacy rule have been deleted in their entirety and there are no longer any mandatory elements for a consent form.

Reason for Elimination of the HIPAA Privacy Consent Form: The Department in eliminating the mandatory HIPAA consent form accomplishes the following according to HHS:

1. Permit all CEs to obtain consent if they choose,
2. Strengthen the notice requirements to preserve the opportunity for individuals to discuss privacy practices and concerns with providers, and
3. Enhance the flexibility of the consent process for those CEs that choose to obtain consent.
4. Other individual rights would not be affected by this proposal.

Remaining Rules:

- MUST STILL FOLLOW THE CE's NPP: Although CEs would not be required to obtain an individual's consent, any uses or disclosure of PHI for TPO would still need to be consistent with the CE's Notice of Privacy Practices.

- *OPTIONAL* CONSENT DOES NOT AFFECT THE "508" AUTHORIZATION PROVISION: The removal of the consent requirement only applies to consent for TPO; it does not alter the requirement to obtain an authorization under 45 CFR 164.508 for uses and disclosures of PHI not otherwise permitted by the privacy rule.

The functions of treatment, payment, and health care operations were given careful consideration according to HHS and HHS intends to strictly enforce the requirement for obtaining an individual's authorization, in accordance with 45 CFR 164.508, for uses and disclosure of PHI for other purposes not permitted or required by the privacy rule. Furthermore, HHS proposes that individuals would retain the right to request restrictions, in accordance with 45 CFR 164.522(a).

Under the proposed modification and as adopted by HHS, a consent could apply only to uses and disclosures that are otherwise permitted by the privacy rule. A consent obtained through this voluntary process would not be sufficient to permit a use or disclosure which, under the privacy rule, requires an authorization or is otherwise expressly conditioned.

The HHS *optional* consent will allow covered entities that choose to have a consent process complete discretion in designing the process.

The most "substantive" corresponding changes were at 45 CFR 164.502 and 164.532. Section 164.502(a)(1) provides a list of the permissible uses and disclosures of PHI, and refers to the corresponding section of the privacy rule for the detailed requirements. HHS proposed to collapse the provisions of 45 CFR 164.502(a)(1)(ii) and (iii) that address uses and disclosures of PHI for TPO and modifies the language to eliminate the consent requirement for these purposes.

The change to permit a CE to use or disclose PHI for these purposes without consent or authorization would apply to any PHI held by a CE whether created or received before or after the compliance date. Therefore, transition provisions would not be necessary.

The HHS also proposed and did effect conforming changes in the definition of "more stringent" to reflect that consent is no longer required.

9. USE OR DISCLOSURE REQUIRING PATIENT AUTHORIZATION:

General Rule: f the covered entity wants an individual's PHI for any reason other than TPO the covered entity must obtain an individual's authorization. A covered entity may not condition treatment, payment or enrollment in a health plan or eligibility for benefits on the individual's signing of an authorization except for research related treatment, enrollment or eligibility prior to the individual's enrollment in a health plan, and payment of claims by a health plan that such disclosure is necessary and does not include the psychotherapy notes.

Psychotherapy Notes: A special category of protected health information, ***psychotherapy notes,*** is generally subject to authorization provision of the final rules, even with respect to treatment, payment or health care operations.

August 2002 modification reference Authorizations: In August 2002 HHS combined the different types of authorizations into a single authorization form. A valid authorization must be written in plain language and be signed by the individual patient and dated. Any authorization has certain "core elements" and "required statements"that are required to be in each authorization. The authorization must contain:

1. A description of the PHI to be used or disclosed;

2. Names of the persons or classes of persons to whom the PHI will be disclosed or from whom such PHI will be requested;

3. Name of the persons or classes of persons authorized to make the requested use or disclosure.

4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure (certain statements are allowed if the authorization is for a use or disclosure of PHI for research or for the creation or maintenance of a research data base or research repository). [SPECIAL NOTE: In Kansas Senate Bill 119 passed in 2002 limits the expiration date to no more than one year from the date of the authorization.]

6. Signature of the individual and date (if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must be recorded on the form).

7. Statement to place the individual on notice of the individual's right to revoke the authorization in writing and either the exceptions to the right to revoke and a description of how the individual may revoke the authorization or to the extent that the information is included in the notice of privacy practice reference to the covered entity's notice of privacy practice.

8. Statement adequate to place the individual on notice of the ability or inability to condition TPO or eligibility for benefits on the authorization by stating either the CE may not condition TPO or eligibility for benefits on whether the individual signs the authorization or when the prohibition on conditioning of authorizations in this section applies or the consequences to the individual for refusal to sign the authorization when, in accordance with the provisions of this section [45 CFR 164.508(b)(4)], the CE can condition treatment, enrollment in a health plan, or eligibility for benefits on failure to obtain such authorization.

9. Statement adequate to place the individual on notice of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the HIPAA privacy rule.

Copy to the Individual: If the CE seeks an authorization from an individual for use or disclosure of PHI the CE must provide the individual with a copy of the signed authorization.

Content of the Authorization Controls: In August 2002 HHS clarified that CEs are required to obtain an authorization for uses and disclosures of PHI unless the use or disclosure is required or otherwise permitted by the HIPAA privacy rule. Accordingly, CEs may only use authorizations that meet the requirements of 45 CFR 164.508(b) and any such use or disclosure will be lawful only to the extent it is consistent with the terms of such authorization. Thus, according to HHS, a voluntary consent document will not constitute a valid permission to use or disclose protected health information for a purpose that requires an authorization under the rule.

Psychotherapy Notes: In the August 2002 preamble to the final rule HHS also clarified the uses and disclosures of psychotherapy notes are such that a CE may not use or disclose psychotherapy notes for purposes of another CE's treatment, payment or health care operations without obtaining the individual's authorization. 67 Fed. Reg. 53220.

Marketing Authorization: A new provision adopted in August 2002 under 45 CFR 164.508(a)(3) requires CEs to obtain an authorization to use or disclose PHI for marketing purposes with two exceptions. (See marketing section for further explanation). The "marketing authority" must have a required additional statement.

Additional Elements Permitted: As with the December 2000 authorization provisions CEs may include additional, non-required elements as long as they are not inconsistent with the required elements and statements now required under 45 CFR 164.508 from the August 2002 revisions.

Invalid Authorization: An authorization is not valid if it contains any of the following defects:

1. The expiration date has passed or the expiration event has occurred, and the CE is aware of the fact;

2. Any of the required core elements or notification statements are omitted or incomplete;

3. The authorization violates the specifications regarding compounding or conditioning authorizations [according to HHS this means that authorizations for the use or disclosure of psychotherapy notes may be combined only with another authorization for the use or disclosure of psychotherapy notes]; or

4. The CE knows that material information in the authorization is false.

Combination with Other Forms: According to HHS in its August 2002 preamble, a CE generally may not combine an authorization with any other type of document, such as the notice of privacy practices or a written voluntary consent. Authorizations may be combined, except for psychotherapy note authorizations as detailed above, unless a CE has conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on one of the authorizations. 45 CFR 164.508(b)(4) needs to be reviewed which in general prohibits the conditioning of treatment, payment, enrollment in a health plan or eligibility for benefits on obtaining an authorization, with the exceptions that are detailed in this section.

Revocation: 45 CFR 164.508(b)(5) provides individuals the right to revoke an authorization any time in writing but an individual may not revoke an authorization if a CE has acted in reliance on the authorization or if the authorization was obtained as a condition of obtaining insurance coverage and other law gives the insurer the right to contest the claim or policy itself.

Record Retention Requirements: Nothing has changed in the August 2002 final privacy rule regarding retention requirements and CEs are required to document and retain authorizations under 45 CFR 164.530(j) for 6 years.

Single Form Created: The different authorization forms identified in the December 2000 final privacy rule have been eliminated and are now consolidated into one set of criteria. CEs may use one authorization form for all purposes.

Authority of Personal Representation: If an individual is signing as a personal representative, the HIPAA privacy rule, according to HHS in its August 2002 preamble, requires that CEs verify and document a person's authority to sign an authorization on an individual's behalf.

Special Authorizations: Other special requirements exist for certain research, marketing and fund raising activities. 45 CFR 164.508 and 65 Fed. Reg. at 82516. "Marketing" is addressed below.

Marketing: In August 2002, HHS eliminated the special provision for marketing health-related products and services originally found at 45 CFR 164.514(e). Now, except as provided for at 45 CFR 164.508(a)(3), a CE must have the individual's prior written authorization to use or disclose PHI for marketing communications and will no longer be able to do so simply by meeting the disclosure and opt-out provisions previously found at 45 CFR 164.514(e). HHS also adopted three categories of communications that are excluded from the definition of "marketing." A CE is not engaged in marketing when it communicates to individuals about: (1) the participating providers in health plans in a network, the services offered by a provider, or the benefits covered by a health plan; (2) the individual's treatment; or (3) case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual. HHS also added language in August 2002 relating to business associate transactions and marketing. Marketing is defined expressly to include "an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service." These communications are marketing and can only occur if the covered entity obtains the individual's authorization pursuant to 45 CFR 164.508.

Under the authorization for marketing requirement, 45 CFR 164.508, the rule expressly requires an authorization for use or disclosure of PHI for marketing communications, except in two circumstances: (1) when the communication occurs in a face-to-face encounter between the covered entity and the individual; or (2) the communication involves a promotional gift of nominal value. Further, a marketing authorization must include a statement about remuneration, if any. It is important to note that the HIPAA privacy marketing provisions do not modify or change any other federal or state law relating to anti-kickback statutes, Stark regulations or self-referral prohibitions. The "marketing" definition excludes communications for the individual's treatment and for case management, care coordination or the recommendation of alternative therapies. Further, HHS clarified that a communication that merely promotes health in a general manner and does not promote a specific product or service from a particular provider does not meet the general definition of "marketing." Therefore, communications such as mailings reminding women to get an annual mammogram, and mailings providing information on how to lower cholesterol, about new developments in health care, about health or "wellness" classes, about support groups, and about health fairs are permitted,

and are not considered marketing. This means that CEs may make communications in newsletter format without authorization so long as the content of such communication is not "marketing," as defined by the rule.

It is important to keep in mind that the marketing authorization exclusion is narrowly crafted to permit only face-to-face encounters between the CE and the individual. HHS has rejected expansion of the face-to-face authorization exception to include telephone, mail, and other common carriers, fax machines or the internet.

10. USE OR DISCLOSURE REQUIREMENT PATIENT OPPORTUNITY TOAGREE OR OBJECT:

General Rule: There are generally three situations where a covered entity may use or disclose PHI without patient consent or authorization ***if*** the patient is given prior notice and a meaningful opportunity to agree or object.

A. A Covered Entity may use or disclose limited general information about patients for creation or maintenance of a ***facility directory***. The requirements relating to a facility directory are very specific. This has been defined as an "opt out" provision in which an individual patient can "opt out" of having their information in a hospital facility directory. If the patient gives permission and information is placed in the facility directory, then only certain types of identifiable information can be disclosed. For the most part the information can only be disclosed if the patient is asked for by name.

Information from a hospital facility directory can be disclosed to a member of the clergy even if the clergy does not ask for the patient by name.

The information that can be included in the facility directory is:

1. The individual patient's name;
2. The individual's present location in the facility that does not describe a level of treatment or care being provided (e.g. behavioral sciences or mental health unit); and
3. General condition of the individual patient (e.g. fair, good, critical).
4. Religious affiliation: The religious affiliation can only be provided to members of the clergy.

If a person inquires at the facility and makes inquiry using the patient's full name then the above first three items can be provided to the individual making the inquiry. This information can be provided, however, only if the individual patient has not opted out of the facility disclosing this information to individuals who make an inquiry. An individual patient may opt out of some but not all of the information.

B. The covered entity may disclose PHI to ***certain relatives, close friends***, or other designees of a patient when it is relevant to that person's ***involvement in the care or payment for care of that patient***.

C. A covered entity may use or disclose PHI to ***notify family members or representatives of a patient of the patient's location, general condition, or death***. The required notice and subsequent agreement or objection may be oral. 45 CFR 164.510.

11. DISCLOSURES PERMITTED WITHOUT WRITTEN AUTHORIZATION:

In certain specific circumstances covered entities are permitted to disclose PHI without obtaining either the optional written consent or an authorization. 45 CFR 164.510 (addressed in Chapter 10) and 512.

The provisions regarding disclosure without authorization have been defined as "highly technical." Compliance with these rules will require covered entities to make a two-step determination before disclosing information:

1. First determine whether a specific situation described in the final rules exists; and;

2. Determine exactly what type of PHI can be disclosed in that particular circumstance.

Covered entities will be permitted to disclose PHI for what has been described as "public policy" purposes. Examples include reporting under state law to disclose communicable diseases, certain abuse situations, vital statistics, health oversight purposes, and in compliance with court and administrative tribunal orders and subpoenas. As indicated above depending on the circumstance there may be additional requirements and the type of the PHI may be limited depending upon the category of the particular circumstance. 45 CFR 164.512.

The final modified privacy rule permits covered entities to disclose PHI, without authorization, to a person subject to the jurisdiction of the FDA for public health purposes relating to the quality, safety, or effectiveness of FDA regulated products or activities such as collecting and reporting adverse events, dangerous products, and defects or problems with FDA regulated products. According to HHS this assures that information will continue to be available to protect public health and safety. 67 Fed. Reg. 53226 - 28

The only other major modification made under 45 CFR 164.512 related to "waiver of authorizations" in the area of research. Such can be reviewed starting at 67 Fed. Reg. 53229. In the revised Final Rule, the Department has retained the minimum necessary requirement for research uses and disclosures made pursuant to Sec. 164.512(i).

12. DISCLOSURE TO BUSINESS ASSOCIATES:

General Rule: A covered entity may generally only disclose PHI to a business associate, or allow a business associate to create or receive such information on its behalf, if the covered entity obtains satisfactory assurance in the form of a written contract that the business associate will appropriately safeguard the information.

Because a business associate generally stands in the shoes of a covered entity with which it has a contract, a restriction agreed to by the covered entity also covers such use or disclosure with respect to the contracted business associate.

Business Associate Contract: The contract must define the boundaries of permissible user disclosure by the business associate, but generally may not allow the business associate to use or disclose the information in a manner that would be a violation of the final privacy rules in the first place, if done by the covered entity.

The contract must also provide, among other things, that the business associate will safeguard against, and report, any unauthorized use or disclosure, and must allow termination by the covered entity if the business associate has violated a material term of the agreement. A covered entity must take reasonable steps to cure any material breach or violation by a business associate with respect to the contract. If unable to cure the breach or violation, the covered entity must terminate the contract if feasible, or otherwise report the breach or violation to The Department of Health and Human Services. 45 CFR 162.502, 504 and 65 Fed. Reg. 82510.

The "sample" HHS business associate contract language can be accessed at http://www.hhs.gov/ocr/hipaa/contractprob.html.

13. PATIENT RIGHT TO NOTICE OF PRIVACY PRACTICES:

General Rule: The final privacy rules require that individuals receive notice regarding the privacy practice of covered entities. 45 CFR 164.520.

The covered entity must provide adequate notice of its permitted uses and disclosures of PHI, the individual's rights and the covered entity's legal obligations with respect to protection of PHI.

The required notice must be written in plain language that includes specific content, such as a detailed description and example for the uses and disclosures permitted or required, and whether the patient's consent or authorization is required.

The covered entity must provide notice to any person upon request, and there are specific requirements for provision of the notice by health plans and certain health care providers both initially and upon revision or change to the notice. Additionally the notice must be posted in a conspicuous place where individuals can review it without request. Specific provisions are also made for electronic notice and joint notice by covered entities participating in organized health care arrangement.

August 2002 modifications reference the Notice of Privacy Practices: In August 2002, HHS adopted a revision to this section of the rule that a covered health care provider with a *direct treatment relationship with an individual* make a good faith effort to obtain the individual's *written acknowledgment of receipt of the notice*. A covered direct treatment provider must make a good faith effort to obtain written acknowledgment no later than the date of first service delivery, including service delivered electronically, that is, at the time the notice is required to be provided. During emergency treatment situations, the final rule at 45 CFR 164.520(c)(2)(i)(B) delays the requirement for provision of the notice until reasonably practicable after the emergency situation, and at 45 CFR 164.520(c)(2)(ii) exempts health care providers from having to make a good faith effort to obtain an individual's acknowledgment in such emergency situations.

Authorization Form Not Designed by HHS: According to HHS, the rule requires only that the acknowledgment be in writing, and does not prescribe other details such as the form that the acknowledgment must take or the process for obtaining the acknowledgment. An example used by HHS is that the final rule does not require an individual's signature to be on the notice. Instead, according to HHS, a covered health care provider is permitted, for example, to have the individual sign a separate sheet or list, or simply initial a cover sheet of the notice to be retained by the provider. Another example used by HHS is that a pharmacist is permitted to have the individual sign or initial an acknowledgment within a log book that patients already sign when they pick up their prescriptions, so long as the individual is clearly informed on the log book that they are acknowledging and the acknowledgment is not also used as a waiver or permission for something else. HHS has stated that it does not consider oral acknowledgment by the individual to be either a

meaningful or appropriate manner by which a covered health care provider may implement the acknowledgment provisions.

"Good Faith" Efforts Must be Recorded if Acknowledgment Form Not Signed: Under the August 2002 modification, if an individual refuses to sign or otherwise fails to provide an acknowledgment, the covered health care provider is required to document its good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained. Accordingly, failure by a CE to obtain an individual's acknowledgment, assuming it otherwise documented its good faith effort, is not a violation of the rule according to HHS.

As indicated above, a CE is required under 45 CFR 164.530(j) to document compliance with the provisions for retaining copies of any written acknowledgments of receipt of the NPP or, if not obtained, documentation of its good faith efforts to obtain such notice.

Example of Non Face to Face Compliance: HHS recognizes that there may be contact between a covered health care provider and an individual that are not face to face. HHS uses the example where a health care provider's first treatment encounter with the patient is over the telephone and can satisfy the notice provision requirements of the rule by mailing the notice to the individual no later than the day of that service delivery. HHS states that to satisfy the requirement that the health care provider also make a good faith effort to obtain the individual's acknowledgment of the notice of privacy practice, the provider may include a "tear-off sheet" or other document with the notice that requests such acknowledgment be mailed back to the provider. HHS also clarifies that when a health care provider's initial contact with the patient is simply to schedule an appointment, the notice provision and acknowledgment requirements may be satisfied at the time the individual arrives at the provider's facility for his or her appointment.

Acknowledgment Form Required Even if Optional Consent Form Still Used: If a covered health care provider elects to continue to use the now optional consent the rule, according to HHS, does not relieve a covered health care provider of his obligations with respect to obtaining an individual's acknowledgment of the notice if that provider also obtains the individual's consent. The rule does provide, however, that those covered health care providers that choose to obtain the optional consent from an individual have the discretion to sign one form that includes both the consent and acknowledgment of the receipt of the notice.

Layered Notice Permitted: The Department also clarifies in August 2002 that covered entities may utilize a "layered notice" to implement the rule's provisions, so long as the elements required by 45 CFR 164.520(b) are included in the document that is provided to the individual. This means, according to HHS, a CE may satisfy the notice provisions by providing the individual with both a shortened notice that briefly summarizes the individual rights, as well as other information; and a longer notice, layered beneath the short notice, that contains all of the elements required by the privacy rule.

New Acknowledgment Form Not Required Unless Patient Requests Revised NPP: In the August 2002 preamble HHS stated that the rule does not require a health care provider to provide any revised notice directly to the individual, unless requested by the individual, and that a new written acknowledgment is not required at the time of revision of the notice.

OCR responds to a question in its December 3, 2002 guidance that a covered health care provider with a direct treatment relationship is not required to obtain a new acknowledgment of receipt of the notice of privacy practices from patients if the facility changes its privacy practice. OCR HIPAA privacy guidance, December 3, 2002, page 108, citing 45 CFR 164.520(c)(2). As an elaboration on this point, in another question and answer format, OCR responds to the following question "Is our medical practice required to notify patients through the mail of any changes to our notice?" The answer is:

> No. The HIPAA Privacy Rule does not require a covered health care provider to mail out its revised notice or otherwise notify patients by mail of changes to the notice. Rather, when a covered health care provider with a direct treatment relationship with individuals makes a change to his notice, he must make the notice available upon request of patients or other persons on or after the effective date of the revision, and, if he maintains a physical service delivery site, post the revised notice in a clear and prominent location in his facility. See 45 CFR 164.520(c)(2)(iv). In addition, the provider must insure that the current notice, in effect at that time, is provided to patients at the first service delivery, and made available on his customer web site, if he has one. See 45 CFR 164.520(c).

OCR HIPAA privacy guidance, December 3, 2002, pages 111-112.

14. PATIENT RIGHTS RELATING TO ACCESS, AMENDMENT AND ACCOUNTING:

GENERAL SUMMARY: The final privacy rule affords patients the right, with limited exceptions, to access, inspect and copy their own PHI. Additionally the rule provides the patient with a right to request an amendment of their PHI and to obtain an accounting of all disclosures of their PHI made by the covered entity within the immediately preceding six-year period. 45 CFR 164.524, 526 and 528.

Covered entities must act within 30 days of a request for access to PHI (if the records are on site) and within 60 days of a request to amend or receive an accounting of PHI. A denial of a patient's request to access or amend PHI must be provided by the covered entity within a specified time period set forth in the final privacy rule, in writing, and must state the reasons for such denial and explain the patient's review rights, if any. A covered entity may not deny a request for an accounting. However, such accounting need not include certain disclosures to include disclosures made to carry out treatment, payment or health care operations, to individuals about their own PHI, or prior to a covered entity's compliance date.

The final modified privacy rule removes from the required disclosures to be included in an accounting all disclosures made pursuant to a signed patient authorization; all disclosed information in a limited data set, and incidental disclosures. The final modified privacy rule also simplifies the accounting for disclosures for research studies. It is recommended that any involvement in a research study, the accounting provision at 45 CFR 164.528 be reviewed in its entirety for determination of what must go in an accounting/accounting log relating to research.

Each of these individual rights (access, amendment and accounting) are addressed in detail in Chapters 16, 17 and 18.

Individual Rights and Business Associates: According to HHS under the Privacy Rule, the CE is responsible for fulfilling all of an individual's rights, including the rights of access, amendment, and accounting, as provided for in 45 CFR 164.524, 164.526, and 164.528. With limited exceptions, a CE is required to provide an individual access to his or her PHI in a designated record set. According to HHS this includes information in a designated record set of a business associate, unless the information held by the business associate merely duplicates the information maintained by the covered entity. However, the Privacy Rule does not prevent the parties from agreeing through the business associate contract that the business associate will provide access to individuals, as may be appropriate where the business associate is the only holder of the, or part of the, designated record set. 67 Fed. Reg. 53253

15. PATIENT RIGHT TO REQUEST ADDITIONAL PRIVACY PROTECTION:

General Rule: An individual has the right to request that the covered entity restrict uses and disclosures of PHI to its own TPO and disclosures to family members or close personal friends involved in the individual's care. 45 CFR 164.522.

A covered entity is not required to agree to such a request. However, if the covered entity agrees to restrict the use or disclosure of PHI as requested the covered entity must then abide by such agreement except in the case of a medical emergency.

HHS in its August 2002 preamble did state that individuals can request confidential forms of communication, even with respect to authorized disclosures, citing to 164.522(b). 67 Fed. Reg. 53189.

HHS has provided guidance in this area of restrictions and possible competing issues:

> However, there are some circumstances in which the Privacy Rule may prohibit a disclosure to a parent or a spouse for payment purposes. For example, under Sec. 164.522(a), an individual has the right to request restrictions to the disclosure of health information for payment. A provider or health plan may choose whether or not to agree to the request. If the covered entity agreed to a restriction, the covered entity would be bound by that restriction and would not be permitted to disclose the individual's health information in violation of that agreement. Also, Sec. 164.522(b) generally requires covered entities to accommodate reasonable requests by individuals to receive communications of protected health information by alternative means or at alternative locations. However, the covered entity may condition the accommodation on the individual providing information on how payment will be handled. In both of these cases, the covered entity has means for permitting disclosures as permitted by the FDCPA [federal Fair Debt Collection Practices Act]. Therefore, these provisions of the Privacy Rule need not limit options available under the FDCPA. However, if the agreed-to restrictions or accommodation for confidential communications prohibit disclosure to a parent or spouse of an individual, the covered entity, and the debt collector as a business associate of the covered entity, would be prohibited from disclosing such information under the Privacy Rule. In such case, because the FDCPA would provide discretion to make a disclosure, but the Privacy Rule would prohibit the disclosure, a covered entity or the debt collector as a business associate of a covered entity would have to exercise discretion granted under the FDCPA in a way that complies with the Privacy Rule. This means not making the disclosure. (See 67 Fed. Reg. 53189)

16. PATIENT RIGHT TO ACCESS HEALTH INFORMATION:

General Rule: Subject to exceptions set forth in the final rule the covered entity must provide a patient access to inspect and obtain a copy of most PHI about the patient maintained by the covered entity.

Psychotherapy Notes: Psychotherapy notes are exempted from the PHI to which a patient has a right to access. Psychotherapy notes are treated differently from other forms of PHI. HHS has commented that psychotherapy notes are highly subjective and sensitive and are deserving of a special higher protected status. The covered entity must obtain patient authorization for any use or disclosure of psychotherapy notes except for use by the originator of the notes for treatment purposes; use or disclosure for training purposes; use or disclosure to defend a legal action brought by the individual; or as otherwise permitted by the final rule for oversight of the psychotherapist. 45 CFR 164.502(a)(2). In addition a covered entity may deny an individual's request to access or amend his or her psychotherapy notes. 45 CFR 164.524(a)(2)(i) and 45 CFR 164.526(a)(2)(iii).

General Requirements: The covered entity may require the patient to make the request in writing, but must grant or deny the request, in whole or in part, in a timely manner.

Any denial of a request must be written in plain language and must state the basis for the denial.

Additionally any denial of a request must describe review rights that are applicable and how to make a complaint to the covered entity or HHS.

When a patient requests review of a reviewable denial, the covered entity's designated reviewing official must determine in a timely manner whether to uphold the denial, and the covered entity must properly notify the patient in writing of the determination.

Costs: When a patient request for access is granted, the covered entity must provide the access in the form requested and in a timely manner, but may impose reasonable cost-based fees for copying, postage, and when agreed to by the patient, preparing a summary of the information. 45 CFR 164.524. This restriction applies only to the individual and not to other who are obtaining the records. 67 Fed. Reg. 53254 (The fee limitations in Sec. 164.524(c)(4) do not apply to any other permissible disclosures by the covered entity, including disclosures that are permitted for treatment, payment or health care operations, disclosures that are based on an individual's authorization that is valid under Sec. 164.508, or other disclosures permitted without the individual's authorization as specified in Sec. 164.512.)

17. PATIENT RIGHT TO REQUEST AMENDMENT OF HEALTH INFORMATION:

General Rule: The covered entity may amend PHI that it maintains about a patient when the patient requests amendment unless the covered entity determines that the information is accurate and complete, was not created or is not maintained by the covered entity (but may have an obligation if previous provider is not available (e.g. deceased) and this covered entity has the previous provider's records), or would not otherwise be available to the patient for inspection.

The covered entity may require the patient to make the amendment request in writing.

Additionally the covered entity may require the patient to provide a reason in support of the request for amendment.

Any denial of an amendment request must be written in plain language and must state the basis for the denial, the patient's right to submit and how to file a written statement disagreeing with the denial, how the patient may request any future disclosures of the information to include the request and denial, and how to make a complaint to the covered entity or HHS.

When a statement of disagreement is submitted, the covered entity must include with future disclosures of the affected information the amendment request, the denial, the statement of disagreement, and any rebuttal statement by the covered entity.

When the covered entity accepts the amendment request, the covered entity must at least identify the affected information and append or provide a link to the amendment.

The covered entity must also notify others holding the affected information of the amendment. Any covered entity receiving such notice must amend the affected information as requested. 45 CFR 164.526.

18. PATIENT RIGHT TO ACCOUNTING OF DISCLOSURES OF HEALTH INFORMATION

General Rule: A covered entity must provide at a patient's request an accounting of all disclosures of the patient's PHI during the six years prior to the request by the CE and its BAs. It should be noted, however, there are several exceptions to this and each exception must be reviewed prior to providing an accounting to the patient.

The accounting must be provided in a timely manner, and generally must include for each disclosure the date, recipient, description, and purpose. The covered entity may not charge a patient for the first accounting requested in any given 12-month period, but may impose a reasonable cost-based fee for any subsequent request in the same 12-month period. 45 CFR 164.528.

August 2002 modification reference Accounting of Disclosures: In August 2002, HHS adopted modifications to eliminate the accounting requirement for authorized disclosures. It is HHS' position that the authorization process itself adequately protects individual privacy by assuring that the individual's permission is given knowingly and voluntarily.

Limited Data Sets Disclosures and Incidental Disclosures Are Not Recorded on an Accounting: In August 2002, HHS added two additional exclusions to the accounting requirements. Disclosures that are part of a *limited data set* and disclosures that are merely *incidental to other permissible uses or disclosures* will not require an accounting. HHS stated that it believed that it is impractical to account for incidental disclosures, which by their very nature, may be uncertain or unknown to the CE at the time they occur. Incidental disclosures, according to HHS, are permitted as long as reasonable safeguards and minimum necessary standards have been observed for the underlying communication. 67 Fed. Reg. 53194 & 53237

Public Policy Disclosures Must be Recorded: HHS in August 2002 did clarify one issue relating to accounting and public purpose disclosures under 45 CFR 164.512. HHS in its August 2002 preamble disagreed with commenters who requested that other public purpose disclosures not be subject to an accounting requirement. HHS recognized that the rule permits disclosures for a variety of public purposes, but such public purpose disclosures are not routine disclosures of the individual's information. The accounting requirement, according to HHS, was designed as a means for the individual to find out the non-routine purpose for which his or her protected health information was disclosed by the CE, so as to increase the individual's awareness of persons or entities other than the individual's health care provider or health plan in possession of this information. To eliminate some or all of these public purpose accounting requirements, according to HHS, would defeat the core purpose of the accounting requirement. Accordingly, public purpose disclosures must be recorded by the CE as an accounting unless it is properly "suspended" under 45 CFR 164.528(a)(2).

A CE must account and therefore record on the accounting provided to any individual disclosures made for public health purposes under 45 CFR 164.512.

Abuse, Neglect and Domestic Violence: In August 2002, HHS also addressed some concerns expressed relating to safety and welfare of victims of abuse, neglect, or domestic violence. HHS gives the covered entity discretion in notifying the victim and/or the individual's personal representative at the time of the disclosure relating to these concerns. If the individual is requesting the accounting, even after being warned of the potential dangers, the CE should honor the request, according to HHS. However, if the request is by the individual's personal representative and the CE has a reasonable belief that such person is the abuser or that providing the accounting to such person could endanger the individual, the CE continues to have the discretion under 45 CFR 164.502(g)(5) to decline such request.

Valid Requests to Temporarily "Suspend" an Accounting: A CE must also comply with any request to suspend an accounting under 45 CFR 164.528(a)(2).

19. PARENTS AS PERSONAL REPRESENTATIVES OF UNEMANCIPATED MINORS:

General Rule: HHS in August 2002 repeated its position that it will continue to defer to state or other applicable law and remain neutral to the extent possible with respect to parents and minors and access by parents to the minor's PHI. In August 2002 HHS added paragraphs to clarify that state and other applicable law governs when such law explicitly requires, permits, or prohibits disclosure of PHI information to a parent. HHS stated that deferring to state or other applicable law includes deference to establish case law as well as an explicit provision in a statute or regulation. HHS made clear that parental access would continue to be subject to any limitations on activities of a personal representative found at 45 CFR 164.502(g)(5) and 45 CFR 164.524(a)(2) and (3). In cases in which the parent is not the personal representative of a minor and state or other law does not require parental access, the HIPAA privacy rule does not provide a parent a right to demand access and does not require a CE to provide access to a parent.

August Clarifications: HHS did adopt "clarifications" and made "changes" in this area. The first "change" relates to disclosure of PHI to a parent In order to assure that State and other applicable laws that address disclosure of health information about a minor to his or her parent govern in all cases, the language in the definition of ``more stringent'' in 45 CFR. 160.202 that addresses the disclosure of PHI about a minor to a parent has been moved to the standards regarding parents and minors in 45 CFR 164.502(g)(3). According to HHS the addition of paragraphs (g)(3)(ii)(A) and (B) of Sec. 164.502, clarify that State and other applicable law governs when such law explicitly requires, permits, or prohibits disclosure of protected health information to a parent.

The second "change" relates to access to PHI. There are two provisions that refer to access, in order to clarify HHS's intent in this area. The first is where there is an explicit State or other law regarding parental access, and the second is where State or other law is silent or unclear, which is often the case with access. Like the provisions regarding disclosure of PHI to a parent, the modified Privacy Rule defers to State or other applicable law regarding a parent's access to health information about a minor. Again, according to HHS the change assures that State or other applicable law governs when the law explicitly requires, permits, or prohibits access to protected health information about a minor to a parent. This includes deference to established case law as well as an explicit provision in a statute or regulation. This issue is addressed in paragraphs (g)(3)(ii)(A) and (B) of 45 CFR 164.502 with the disclosure provisions the final modifications also clarify that, the discretion to provide or deny access to a parent under 45 CFR164.502(g)(3)(ii)(C) only may be exercised by a licensed health care professional, in the exercise of professional judgment. (See 67 Fed. Reg. 53200-01)

20. MARKETING

General Rule: The privacy rule requires an individual's written authorization before a use or disclosure of PHI can be made for marketing. The rule does, however, distinguish between marketing communications from those communications about goods and services that are essential for quality health care.

New Definition: The final privacy rule defines "marketing" as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." OCR HIPAA privacy guidance, December 3, 2002, page 65. If the communication is marketing, then the communication can occur only if the covered entity first obtains an individual's written authorization. Examples provided by OCR are as follows:

- A communication from a hospital informing former patients about a cardiac facility, that is not part of the hospital, that can provide a base line EKG for $39.00, when the communication is not for the purpose of providing treatment advice. OCR HIPAA privacy guidance, December 3, 2002, page 65.

A second type of "marketing" is any "arrangement between a covered entity and another entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service." As explained by OCR this part of the definition of marketing has no exceptions. The individual must authorize these types of marketing communications before they can occur. OCR HIPAA privacy guidance, December 3, 2002, page 66. An example provided by OCR is that a drug manufacturer receives a list of patients from a covered health care provider and provides remuneration. Then, uses that list to send discount coupons for a new anti-depressant medication directly to the patients. This is considered the type of marketing that requires previous written authorizations. OCR has opined that covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list. OCR HIPAA privacy guidance, December 3, 2002, page 66.

Exceptions to Marketing: OCR in its December 2002 guidance also explains what is not marketing. Three exceptions apply to the definition of marketing:

1. A communication is not marketing if it is made to describe a health-related 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 entity's participating in a health care provider network or a health plan network, replacement of or enhancements to a health plan; and health-related products or services available only to a health plan enrollee that adds value to, but are not part of, a plan for benefits.

2. A communication is not marketing if it is made for treatment and made to the individual with examples described by OCR as a pharmacy or other health care provider who mails prescription reminders to patients, or contracts with a mail house to do so or a primary care physician refers an individual to a specialist for a follow-up test or provides free samples of a prescription drug to a patient.

3. A communication is not marketing if it is made for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. In this third category, examples are an endocrinologist shares a patient's medical record with several behavior management programs to determine which program best suits the ongoing needs of the individual patient or a hospital social worker shares medical record information with various nursing homes in the course of recommending the patient be transferred from a hospital bed to a nursing home.

OCR HIPAA privacy guidance, December 3, 2002, pages 66-67.

OCR states explicitly that for any of the three exceptions to the definition of marketing, the specific activity must otherwise be permissible under the HIPAA privacy rule. OCR HIPAA privacy guidance, December 3, 2002, page 67.

Face to Face Communications: A communication, however, does not require an authorization, even if it is marketing, if it is in the form of a face-to-face communication made by a covered entity to an individual; or if it is a promotional gift of nominal value provided by the covered entity. An example provided by OCR when no prior authorization is necessary is when a hospital provides a free package of formula and other baby products to new mothers as they leave the maternity ward. OCR HIPAA privacy guidance, December 3, 2002, page 68.

Prescriptions Refills: It is important to note that OCR indicates that a doctor or pharmacy can be paid to make a prescription refill reminder without a prior authorization even if a third party pays for the communication. According to OCR the prescription refill reminder is considered treatment. Accordingly, that communication is excluded from the definition of marketing and does not require prior authorization. OCR HIPAA privacy guidance, December 3, 2002, page 73.

Application to Other Federal Laws - Anti-Kickback, Fraud & Abuse, or Self-Referral: An important component of the HIPAA marketing provisions is that it is not to be construed as amending, modifying, or changing any rule or requirement related to any other federal or state statutes or regulations including specifically anti-kickback, fraud and abuse, or self referral statutes or regulations or to authorize or permit any activity or transaction currently proscribed by such statutes and regulations. OCR HIPAA privacy guidance, December 3, 2002, page 75. The definition of "marketing" under the HIPAA privacy rule relates to the HIPAA privacy rule standards only. OCR states with particularity that although the HIPAA privacy rule defines the term "marketing" to exclude communications to an individual to recommend, purchase, or use a product or service as

part of the treatment of the individual or for case management or care coordination of that individual, such communication by a health care provider may violate the anti-kickback statute. OCR states that even if the privacy rule requires written authorization because it is "marketing" under the HIPAA privacy rule, such arrangement may nevertheless violate other statutes and regulations administered by the Department of Health and Human Services, Department of Justice, or other federal or state agencies. OCR HIPAA privacy guidance, December 3, 2002, page 75-76.

21. GENERAL ADMINISTRATIVE COMPLIANCE ISSUES:

The final privacy rule imposes numerous administrative requirements on a covered entity to ensure compliance with the rule's privacy and access provisions.

Initially a covered entity must designate a privacy official responsible for the development and implementation of the entity's policies and procedures for compliance.

Additionally a covered entity must designate a contact person or office responsible for providing information, receiving complaints about privacy and access matters, and to field questions relative to an entity's "notice of privacy practices." A Covered Entity must also maintain a record of who will process access, amendment and accounting requests.

A covered entity must also train each member of its workforce on its policies and procedures as they relate to that member's functions. This applies to both new workforce members and existing workforce members. Additionally ongoing training is to be provided.

A covered entity must take steps to mitigate any breach of the safeguards or other violations of its policies and procedures with respect to PHI.

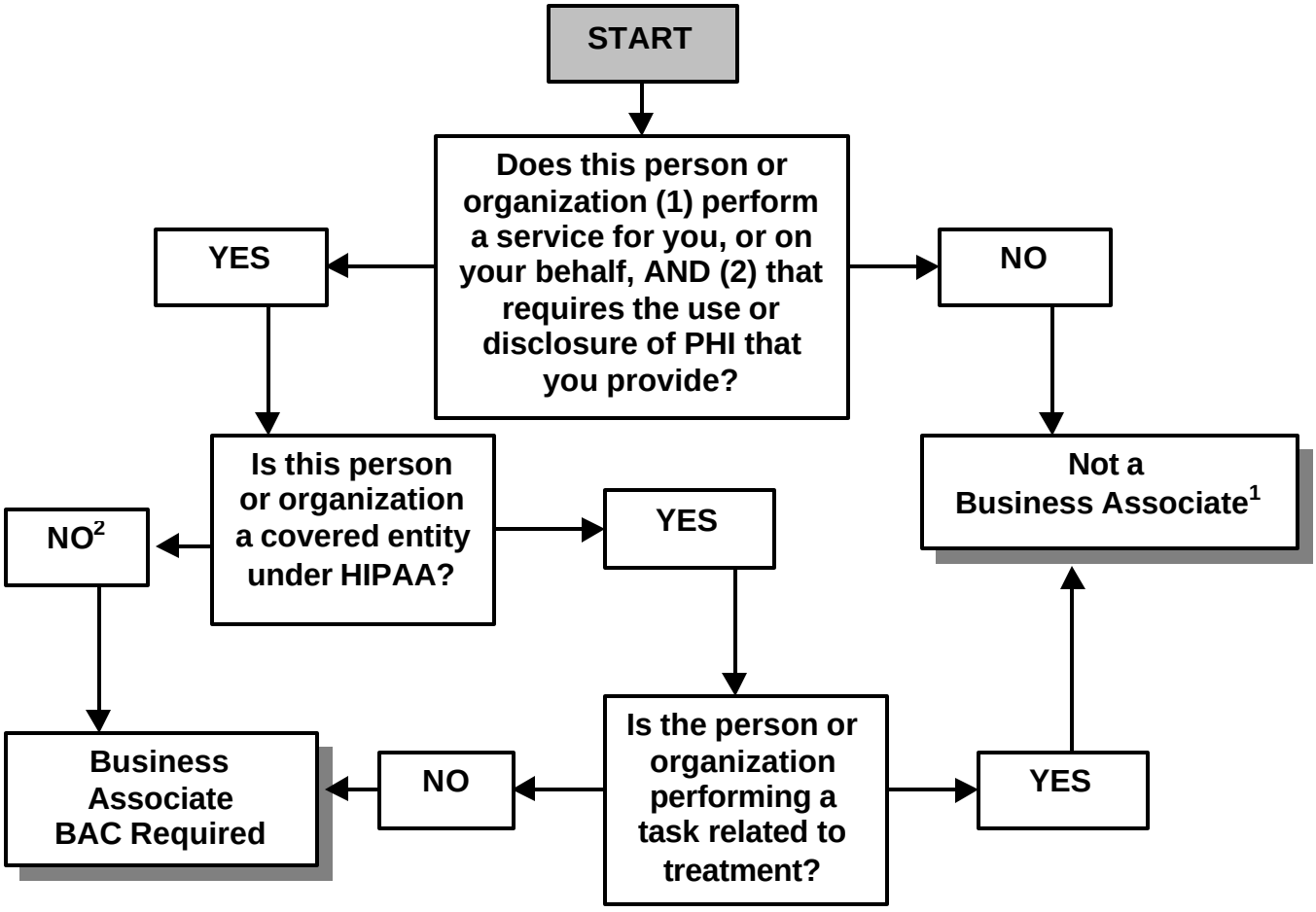
A covered entity must document its policies and procedures and all other aspects of its compliance with the privacy rules. 45 CFR 164.530.

Covered entities, being required to develop and implement polices to establish compliance with the final rules, must carefully review 45 CFR 164.530(c)-(i) requirements. Covered entities should have policies on the following: (see the attached POLICY CHECKLIST)

- Designation of Personnel
- Notice of Privacy Practices and Acknowledgment
- Individual Rights
- Training
- Use and Disclosure of TPO
- Disclosures for Public Policy Purposes
- Verification Procedures
- Request for Restrictions & Alternative Communications
- Discipline
- Routine and Recurring Disclosures
- Non-routine and Recurring Disclosures
- Authorizations
- Facility Directories & Disclosures to Clergy, Family and Friends
- Designated Record Set
- Administrative Requirements

BUSINESS ASSOCIATE
"GENERAL RULE" DECISION CHART

Begin your analysis with "START."
Answer each question and follow line from the answer box to determine if the person or entity is a "business associate."



[1] (*e.g.* copier service technicians, janitors, mail/package couriers, & health care providers involved in providing treatment to a patient and the health care provider has privileges at the hospital.)

[2] Some health care providers may not meet the definition of a covered entity [CE] because they do not engage in an electronic transaction. In such a case no BAC is needed if the PHI is provided as part of treatment AND you include the person as part of your "workforce" definition (*e.g.* independent contractors).

Decision Tree to Assist with Business Associate Analysis

Consider the following if a Covered Entity Wants To provide PHI to you or if you want a Covered Entity to send PHI to you.