

# HIPAA Privacy

*An innovative approach to self-implementation*

# WorkGroups<sup>®</sup>

## Teleconference

# Self-Insured Employer Compliance

---

## Building on Provider Compliance Efforts

*[Ver 1.0]*

## Rules and Resources

Wednesday, January 28, 2004  
10:00 a.m. – 11:00 a.m., CST



## Outline

I.	Background	2
	A. Who is covered?	2
	B. Discussion	5
	C. Compliance dates	6
	D. Specific transaction requirements	9
II.	Summary of Obligations of Employers as Plan Sponsors	10
	A. Assurances the Employer Must Give to the Health Plan	10
	B. Amendment of Plan Documents.	10
	C. Prevention of Disclosure or Use for Other Purposes.	11
	D. Fully Insured vs. Self Insured Health Plans.	12
III.	Organizational Requirements	13
VI.	Privacy Rule Requirements	16
V.	Security Rule Requirements	30
VI.	Comparison of Provider and Health Plan Policies	31
VII.	Final Thoughts	37

### Session Description

The compliance deadline for small health plans (including most self-insured healthcare providers) is April 14, 2004. This new one-hour session will review how providers can use their existing compliance efforts (policies, forms, etc.) to streamline their health plan requirements.

## I. Background

### A. Who is covered?

---

#### § 160.102 Applicability.

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

§ 160.103 Definitions.<sup>1</sup> Except as otherwise provided, the following definitions apply to this subchapter:

\* \* \*

*Covered entity* means:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

\* \* \*

*Group health plan* (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg– 91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

- (1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
- (2) Is administered by an entity other than the employer that established and maintains the plan.

---

<sup>1</sup> Security Rule changes to this section discussed generally in the Preamble, 68 FR 8334, 8339.

\* \* \*

*Health insurance issuer* (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

*Health maintenance organization (HMO)* (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of *health plan* in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

*Health plan* means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

- (i) A group health plan, as defined in this section.
- (ii) A health insurance issuer, as defined in this section.
- (iii) An HMO, as defined in this section.
- (iv) Part A or Part B of the Medicare program under title XVIII of the Act.
- (v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, *et seq.*
- (vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
- (vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
- (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
- (ix) The health care program for active military personnel under title 10 of the United States Code.
- (x) The veterans health care program under 38 U.S.C. chapter 17.
- (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).
- (xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*
- (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, *et seq.*
- (xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, *et seq.*
- (xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

\* \* \*

*Organized health care arrangement*<sup>2</sup> means:

\* \* \*

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;<sup>3</sup>

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor;<sup>4</sup> or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.<sup>5</sup>

\* \* \*

<sup>2</sup> Moved from 45 CFR § 164.501 at 68 FR 8374 (February 20, 2003).

<sup>3</sup> “The Department clarifies that, if more than summary health information is needed for this purpose, paragraphs (3), (4), and (5) of the definition of “organized health care arrangement” may permit the disclosure. These provisions define the arrangements between group health plans and their health insurance issuers or HMOs as OHCA, which are permitted to share information for each other’s health care operations. Such disclosures also may be made to a broker or agent that is a business associate of the health plan. The Department clarifies that the OHCA provisions also permit the sharing of protected health information between such entities even when they no longer have a current relationship, that is, when a group health plan needs protected health information from a former issuer..” Preamble to final revisions, 67 FR 53217-18

<sup>4</sup> *Ibid.*

<sup>5</sup> *Ibid.*

*Small health plan* means a health plan with annual receipts of \$5 million or less.

\* \* \*

## **B. Discussion**

---

### **A. Since employers are not “Covered Entities” under the HIPAA Privacy Rules, why should employers be concerned about compliance?**

The HIPAA Privacy Rules treat employers and the group health plans that they sponsor as two separate legal entities. In order for the employer to receive and use PHI from the group health plan it sponsors, the employer must amend the group health plan document to include provisions in which the employer agrees to comply with the Privacy Rules.

A “group health plan” is defined as an employee welfare benefit plan as defined in Section 3(1) of the Employee Retirement Income Security Act of 1974 (“ERISA”), including insured and self-insured plans, that provides medical care to employees or their dependents that has at least fifty (50) participants and is administered by an entity other than the employer that established and maintains the plan.

For employers who sponsor fully-insured group health plans, the employer can escape most of the requirements of the Privacy Rules -- except the requirements for no retaliation and no waiver of rights -- by simply refusing to receive any PHI from the health insurance carrier who insures the plan. Employers that sponsor self-insured group health plans, however, do not have this option.

### **B. Are fully insured health plans that do not handle PHI exempt from compliance with the HIPAA Privacy Rules?**

No. This is a common misconception. Fully insured health plans that do not receive PHI still have some limited HIPAA Privacy Rule responsibilities, such as the prohibitions on retaliation and waiver of rights. In this case, the insurer rather than the plan is required to maintain the notice of privacy practices.

### **C. Types of health plans covered by HIPAA Privacy Rules:**

- Medical
- Dental
- Vision
- Employee Assistance Program (EAP) (unless EAP operates merely as referral source)
- Medical flexible spending accounts
- Long-term care plans
- On-the-job injury plans for employers who have “opted out” of a state workers’ compensation system and who have created an ERISA plan to deal with on-the-job injuries

## C. Compliance Dates

---

### What is a small health plan?

**“Question:** HIPAA allows "small health plans, " defined as health plans having annual receipts of \$5 million or less, an additional year (in the case of the Privacy Rule, until April 14, 2004) to come into compliance. How should a health plan determine what receipts to use to decide whether it qualifies as a "small health plan?"

**Answer:** Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 CFR 121.104 to calculate annual receipts. Health plans that do not report receipts to the IRS - for example, ERISA group health plans that are exempt from filing income tax returns - should use proxy measures to determine their annual receipts. Further information about the relevant provisions of 13 CFR 121.104 and these proxy measures, and additional information related to “small health plans,” may be found at <http://cms.hhs.gov/hipaa/hipaa2/default.asp>.” (OCR FAQ Answer ID 368, 03/03/2003)

### 13 CFR 121.104 How does SBA calculate annual receipts?

(a) Definitions. In determining annual receipts of a concern:

(1) Receipts means “total income” (or in the case of a sole proprietorship, “gross income”) plus “cost of goods sold” as these terms are defined or reported on Internal Revenue Service (IRS) Federal tax return forms; Form 1120 for corporations; Form 1120S for Subchapter S corporations; Form 1065 for partnerships; and Form 1040, Schedule F for farm or Schedule C for sole proprietorships). However, the term receipts excludes net capital gains or losses, taxes collected for and remitted to a taxing authority if included in gross or total income, proceeds from the transactions between a concern and its domestic or foreign affiliates (if also excluded from gross or total income on a consolidated return filed with the IRS), and amounts collected for another by a travel agent, real estate agent, advertising agent, conference management service provider, freight forwarder or customs broker.

(2) Completed fiscal year means a taxable year including any short period. Taxable year and short period have the meaning attributed to them by the IRS.

(3) Unless otherwise defined in this section, all terms shall have the meaning attributed to them by the IRS.

(b) Period of measurement.

(1) Annual receipts of a concern which has been in business for 3 or more completed fiscal years means the receipts of the concern over its last 3 completed fiscal years divided by three.

(2) Annual receipts of a concern which has been in business for less than 3 complete fiscal years means the receipts for the period the concern has been in business divided by the number of weeks in business, multiplied by 52.

(3) Annual receipts of a concern which has been in business 3 or more complete fiscal years but has a short year as one of those years means the receipts for the short year and the two full fiscal years divided by the number of weeks in the short year and the two full fiscal years, multiplied by 52.

(c) Use of information other than the Federal tax return. Where other information gives SBA reason to regard Federal Income Tax returns

as false, SBA may base its size determination on such other information.

(d) Annual receipts of affiliates.

(1) If a concern has acquired an affiliate or been acquired as an affiliate during the applicable averaging period or before small business self-certification, the annual receipts in determining size status include the receipts of both firms. Furthermore, this aggregation applies for the entire applicable period used in computing size rather than only for the period after the affiliation arose. Receipts are determined for the concern and its affiliates in accordance with paragraph (b) of this section even though this may result in different periods being used to calculate annual receipts.

(2) The annual receipts of a former affiliate are not included as annual receipts if affiliation ceased before the date used for determining size. This exclusion of annual receipts of a former affiliate applies during the entire period used in computing size, rather than only for the period after which the affiliation ceased .

### Subpart I—General Provisions for Transaction

#### § 162.900—Compliance dates of the initial implementation of the code sets and transaction standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of subparts I through N of this part no later than October 16, 2002.

(b) *Health plans.* A health plan must comply with the applicable requirements of subparts I through R of this part no later than one of the following dates:

(1) *Health plans other than small health plans*— October 16, 2002.

(2) *Small health plans*— October 16, 2003.

(c) *Health care clearinghouses.* A health care clearinghouse must comply with the applicable requirements of subparts I through R of this part no later than October 16, 2002.

### HIPAA Administrative Simplification Compliance Act (ASCA) Frequently Asked Questions

\* \* \*

#### **Q3: Can small health plans get an extension to their current compliance date of October, 2003?**

A3: No, the compliance date for small plans does not change.

#### § 164.534 Compliance dates for initial implementation of the privacy standards.

(a) *Health care providers.* A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) *Health plans.* A health plan must comply with the applicable requirements of this subpart no later than the following date, as applicable:

(1) *Health plans other than small health plans* April 14, 2003.

(2) *Small health plans* April 14, 2004.

(c) *Health care clearinghouses*. A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003

### § 164.532 Transition provisions.

\* \* \*

(d) *Standard: Effect of prior contracts or other arrangements with business associates*. Notwithstanding any other provisions of this subpart, a covered entity, other than a small health plan, may disclose protected health information to a business associate and may allow a business associate to create, receive, or use protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.502(e) and 164.504(e) consistent with the requirements, and only for such time, set forth in paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance*.

(1) *Qualification*. Notwithstanding other sections of this subpart, a covered entity, other than a small health plan, is deemed to be in compliance with the documentation and contract requirements of §§ 164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to October 15, 2002, such covered entity has entered into and is operating pursuant to a written contract or other written arrangement with a business associate for such business associate to perform functions or activities or provide services that make the entity a business associate; and

(ii) The contract or other arrangement is not renewed or modified from October 15, 2002 until the compliance date set forth in § 164.534.

(2) *Limited deemed compliance period*. A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section, shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after the compliance date set forth in § 164.534; or

(ii) April 14, 2004.

(3) *Covered entity responsibilities*. Nothing in this section shall alter the requirements of a covered entity to comply with Part 160, Subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

### Sec. 164.318 Compliance dates for the initial implementation of the security standards.

(a) Health plan.

(1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) Health care clearinghouse. A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) Health care provider. A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

## **D. Specific Transaction Compliance Requirements**

### **§ 162.925 Additional requirements for health plans.**

(a) *General rules.*

(1) If an entity requests a health plan to conduct a transaction as a standard transaction, the health plan must do so.

(2) A health plan may not delay or reject a transaction, or attempt to adversely affect the other entity or the transaction, because the transaction is a standard transaction.

(3) A health plan may not reject a standard transaction on the basis that it contains data elements not needed or used by the health plan (for example, coordination of benefits information).

(4) A health plan may not offer an incentive for a health care provider to conduct a transaction covered by this part as a transaction described under the exception provided for in § 162.923(b).

(5) A health plan that operates as a health care clearinghouse, or requires an entity to use a health care clearinghouse to receive, process, or transmit a standard transaction may not charge fees or costs in excess of the fees or costs for normal telecommunications that the entity incurs when it directly transmits, or receives, a standard transaction to, or from, a health plan.

(b) *Coordination of benefits.* If a health plan receives a standard transaction and coordinates benefits with another health plan (or another payer), it must store the coordination of benefits data it needs to forward the standard transaction to the other health plan (or other payer).

(c) *Code sets.* A health plan must meet each of the following requirements:

(1) Accept and promptly process any standard transaction that contains codes that are valid, as provided in subpart J of this part.

(2) Keep code sets for the current billing period and appeals periods still open to processing under the terms of the health plan's coverage.

## II. Summary of Obligations of Employers as Plan Sponsors

Because the HIPAA Privacy Rules treat employers and the group health plans that they sponsor as two separate legal entities, and, consequently, a plan sponsor is not a “covered entity” per se, the HIPAA Privacy Rules mandated ways for PHI to be exchanged between the group health plans and their sponsors. Essentially, the employer sponsoring the group health plan must agree to comply with the same Privacy Rules that the health plan must follow. This is accomplished through an amendment to the plan documents.

### A. Assurances the Employer Must Give to the Health Plan

1. A group health plan that is a covered entity may only disclose PHI to a plan sponsor, or provide for or permit the disclosure of PHI to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, if the plan sponsor amends plan documents to restrict uses and disclosures of PHI.
2. In order to obtain PHI from the health plan, the plan sponsor must certify to the health plan that the plan documents have been amended and the plan sponsor agrees to the restricted uses and disclosures contained therein.
3. With such a plan amendment and the assurances contained therein, a health plan may disclose PHI to a plan sponsor only to the extent such information is needed by the plan sponsor to perform its administrative functions.
  - a. However, a health plan may not permit a health insurer or HMO to disclose PHI to a plan sponsor except as permitted by the Privacy Rules.
  - b. In addition, a health plan may not disclose PHI to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.
4. Exceptions to the plan amendment requirements:
  - a. Exception: A health plan may disclose summary health information to the plan sponsor if the information is requested:
    - (i) to obtain premium bids from health plans for providing health insurance coverage under the plan, or
    - (ii) to modify, amend or terminate the plan.
  - b. Exception: A health plan may disclose information on whether the individual is participating in the group health plan or is enrolled or disenrolled from a health insurance issuer or HMO offered by the plan to the plan sponsor.

### B. Amendment of Plan Documents.

The plan documents of the group health plan must be amended to incorporate the following provisions.

1. The plan document should establish the permitted and required uses and disclosures of PHI by the plan sponsor consistent with the requirements of the Privacy Rules.

2. The plan document should provide that the health plan will disclose PHI to the plan sponsor only upon receipt of certification by the plan sponsor that the plan documents have been amended and the plan sponsor agrees to:
  - a. refrain from using or disclosing PHI other than as permitted or required by the plan documents or law;
  - b. ensure that any agents to whom it provides PHI received from the health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to PHI;
  - c. refrain from using or disclosing PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
  - d. report to the health plan any use or disclosure of PHI that is inconsistent with the uses and disclosures for which the information was provided;
  - e. make PHI available to individuals;
  - f. allow amendment of PHI and incorporate such amendment;
  - g. allow individuals to request an accounting of disclosures of PHI;
  - h. make its internal practices, books and records relating to the use and disclosure of PHI received from the health plan available to the HHS;
  - i. return or destroy all PHI received from the health plan that the plan sponsor maintains in any form and retain no copies of the information for a period no longer than needed for the purpose of the disclosure (if return or destruction is not feasible, then further uses and disclosures shall be prohibited, limited only to those purposes making return or destruction infeasible); and
  - j. ensure adequate separation between the health plan and the plan sponsor by:
    - (i) describing those employees or classes of employees other than persons under the control of the plan sponsor to be given access to PHI (any employee who receives PHI relating to payment under, health care operations of, or other matters pertaining to the health plan in the ordinary course of business must be included in the description);
    - (ii) restricting their use and access to plan administration functions that the plan sponsor performs for the health plan; and
    - (iii) providing an effective mechanism for resolving any issues of noncompliance by persons with access to such information.

**C. Prevention of Disclosure or Use for Other Purposes.**

1. Amendment of the plan documents permits disclosure to the extent such information is needed by the plan sponsor to perform its administrative functions.
2. Without a plan amendment, disclosure is only permitted in the above described instances: (1) disclosure of summary health information, and (2) disclosure of enrollment/disenrollment information.

**D. Fully Insured vs. Self Insured Health Plans.**

---

1. Fully insured group health plans.
  - a. If an employer sponsors a fully insured group health plan, it can escape the plan amendment requirements by declining to receive PHI. In that instance, the employer can still receive summary health information and enrollment information.
  - b. The employer, if it declines to receive PHI, can also escape the other requirements of the Privacy Rules.
  - c. Exception: Employers who sponsor fully insured group health plans cannot escape the requirements for no retaliation and no waiver of rights.
  
2. Self-insured group health plans.
  - a. If an employer sponsors a self-insured group health plan, it can also escape the plan amendment requirements by declining to receive PHI.
  - b. However, the sponsor of a self-insured group health plan cannot escape the other requirements of the Privacy Rules, including, but not limited to, having a privacy officer, following the privacy procedures, providing training, etc.

### III. Organizational Requirements

**Sec. 164.103 Definitions.**<sup>6</sup> As used in this part, the following terms have the following meanings:

*Common control*<sup>7</sup> exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

*Common ownership*<sup>8</sup> exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

*Covered functions*<sup>9</sup> means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

*Health care component*<sup>10</sup> means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with Sec. 164.105(a)(2)(iii)(C).

*Hybrid*<sup>11</sup> entity means a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and
- (3) That designates health care components in accordance with paragraph Sec. 164.105(a)(2)(iii)(C).

*Plan sponsor*<sup>12</sup> is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

\* \* \*

#### **Sec. 164.105 Organizational requirements.**

(a) (1) *Standard: Health care component.*<sup>13</sup> If a covered entity is a hybrid entity, the requirements of subparts C and E of this part, other than the requirements of this section, Sec. 164.314, and Sec. 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) *Implementation specifications:*<sup>14</sup>

(i) *Application of other provisions.* In applying a provision of subparts C and E of this part, other than the requirements of this section, Sec. 164.314, and Sec. 164.504, to a hybrid entity:

---

<sup>6</sup> Added 68 FR 8334, 8374-5 (February 20, 2003).

<sup>7</sup> Moved from 45 CFR 164.504 at 68 FR 8334, 8374 (February 20, 2003).

<sup>8</sup> Moved from 45 CFR 164.504 at 68 FR 8334, 8375 (February 20, 2003).

<sup>9</sup> Moved from 45 CFR 164.500 at 68 FR 8334, 8375 (February 20, 2003).

<sup>10</sup> Moved from 45 CFR 164.504 at 68 FR 8334, 8375 (February 20, 2003).

<sup>11</sup> Moved from 45 CFR 164.504 at 68 FR 8334, 8375 (February 20, 2003).

<sup>12</sup> Moved from 45 CFR 164.500 at 68 FR 8334, 8375 (February 20, 2003).

<sup>13</sup> Replaces 45 CFR 164.504(b).

<sup>14</sup> Replaces 45 CFR 164.504(c)(1).

(A) A reference in such provision to a "covered entity" refers to a health care component of the covered entity;

(B) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse," refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to "protected health information" refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to "electronic protected health information" refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) *Safeguard requirements.*<sup>15</sup> The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this section and subparts C and E of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by subpart E of this part;

(D) A component that is described by paragraph (a)(2)(iii)(C)(2) of this section that creates, receives, maintains, or transmits electronic protected health information on behalf of the health care component is in compliance with subpart C of this part; and

(E) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.*<sup>16</sup> A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with subpart E of this part.

<sup>15</sup> Replaces 45 CFR 164.504(c)(2).

<sup>16</sup> Replaces 45 CFR 164.504(c)(3).

(B) The covered entity is responsible for complying with Sec. 164.316(a) and Sec. 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this section and subparts C and E of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(1) Covered functions; or

(2) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

(b) (1) *Standard: Affiliated covered entities.*<sup>17</sup> Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of subparts C and E of this part.

(1) Implementation specifications:

(i) Requirements for designation of an affiliated covered entity.

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of subparts C and E of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) Safeguard requirements. An affiliated covered entity must ensure that:

(A) The affiliated covered entity's creation, receipt, maintenance, or transmission of electronic protected health information complies with the applicable requirements of subpart C of this part;

(B) The affiliated covered entity's use and disclosure of protected health information comply with the applicable requirements of subpart E of this part; and

(C) If the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, the affiliated covered entity complies with Sec. 164.308(a)(4)(ii)(A) and Sec. 164.504(g), as applicable.

(c) (1) *Standard: Documentation.* A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) *Implementation specification: Retention period.* A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

---

<sup>17</sup> Replaces 45 CFR 164.504(d).

## IV. Privacy Rule Requirements

§ 164.501 Definitions.<sup>18</sup> As used in this subpart, the following terms have the following meanings:

\* \* \*

*Designated record set* means:

(1) A group of records maintained by or for a covered entity that is:

- (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
- (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

\* \* \*

*Health care operations* means any of the following activities of the covered entity to the extent that the activities are related to covered functions:<sup>19</sup>

- (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities<sup>20</sup>; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

---

<sup>18</sup> In 45 CFR §164.501, the definitions of the following terms were removed and added to 45 CFR §160.103 at 68 FR 8334, 8381 (February 20, 2003):, Disclosure, Individual, Organized health care arrangement, Protected health information, and Use. The definitions of the following terms were removed and added to 45 CFR §164.103: Covered functions, Plan sponsor Required by law.

<sup>19</sup> Before the August 14, 2002 amendments, this introduction read: “*Health care operations* means any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:”

<sup>20</sup> “A study with such a purpose would meet the rule’s definition of research, and use or disclosure of protected health information would have to meet the requirements of §§ 164.508 or 164.512(i).” (Preamble page 82490)

- (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
- (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- (6) Business management and general administrative activities of the entity, including, but not limited to:
- (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
  - (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
  - (iii) Resolution of internal grievances;
  - (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity;<sup>21</sup> and
  - (v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.<sup>22</sup>

*Health oversight agency* means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

\* \* \*

*Marketing* means<sup>23</sup>:

<sup>21</sup> Before the August 14, 2002 amendment, Paragraph (6)(iv) read as follows: “Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and”.

<sup>22</sup> Before the August 14, 2002 amendment, Paragraph (6)(v) read as follows: “Consistent with the applicable requirements of § 164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).” The Preamble to the December 28, 2002 rule noted at page 82491 regarding this section as follows: “For example, under this category we permit uses or disclosures of protected health information to determine from whom an authorization should be obtained, for example to generate a mailing list of individuals who would receive an authorization request.”

<sup>23</sup> “The Department does not agree that the simple receipt of remuneration should transform a treatment communication into a commercial promotion of a product or service. For example, health care providers should be able to, and can, send patients prescription

(1) To make a communication about a product or service that encourages<sup>24</sup> recipients of the communication to purchase or use<sup>25</sup> the product or service, unless the communication is made:

(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or 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 add value to, but are not part of, a plan of benefits.<sup>26</sup>

(ii) For treatment<sup>27</sup> of the individual; or

(iii) 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.

---

refill reminders regardless of whether a third party pays or subsidizes the communication. The covered entity also is able to engage a legitimate business associate to assist it in making these permissible communications. It is only in situations where, in the guise of a business associate, an entity other than the covered entity is promoting its own products using protected health information it has received from, and for which it has paid, the covered entity, that the remuneration will place the activity within the definition of ‘marketing.’” August 14, 2002 Revisions, 67 Fed. Reg. 53187.

“Covered entities may make communications in newsletter format without authorization so long as the content of such communications is not “marketing,” as defined by the Rule. The Department is not creating any special exemption for newsletters.” August 14, 2002 Revisions, 67 Fed. Reg. 53187.

“[N]othing in the marketing provisions of the Privacy Rule are 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. ... Although a particular communication under the Privacy Rule may not require patient authorization because it is not marketing, or may require patient authorization because it is “marketing” as the Rule defines it, the arrangement may nevertheless violate other statutes and regulations administered by HHS, the Department of Justice, or other Federal or State agency.” August 14, 2002 Revisions, 67 Fed. Reg. 53187-8.

<sup>24</sup> “If, on its face, the communication encourages recipients of the communication to purchase or use the product or service, the communication is marketing. ... Tying the definition of “marketing” to the purpose of the communication creates a subjective standard that would be difficult to enforce because the intent of the communicator rarely would be documented in advance. The definition adopted by the Secretary allows the communication to speak for itself.” August 14, 2002 Revisions, 67 Fed. Reg. 53186.

<sup>25</sup> The Department clarifies 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.” Such communications may include population-based activities to improve health or reduce health care costs as set forth in the definition of “health care operations” at §164.501. Therefore, communications, such as mailings reminding women to get an annual mammogram, and mailings providing information about how to lower cholesterol, about new developments in health care (e.g., new diagnostic tools), about health or “wellness” classes, about support groups, and about health fairs are permitted, and are not considered marketing. August 14, 2002 Revisions, 67 Fed. Reg. 53189.

<sup>26</sup> “[U]nder this exemption, a health plan is not engaging in marketing when it advises its enrollees about other available health plan coverages that could enhance or substitute for existing health plan coverage. For example, if a child is about to age out of coverage under a family’s policy, this provision will allow the plan to send the family information about continuation coverage for the child. This exception, however, does not extend to excepted benefits (described in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1)), such as accident-only policies), nor to other lines of insurance (e.g., it is marketing for a multi-line insurer to promote its life insurance policies using protected health information)... To qualify for this exclusion, however, the [value-added items or services] must meet two conditions. First, they must be health-related. Therefore, discounts offered by Medicare + Choice or other managed care organizations for eyeglasses may be considered part of the plan’s benefits, whereas discounts to attend movie theaters will not. Second, such items and services must demonstrably “add value” to the plan’s membership and not merely be a pass-through of a discount or item available to the public at large. Therefore, a Medicare + Choice or other managed care organization could, for example, offer its members a special discount opportunity for a health/fitness club without obtaining authorizations, but could not pass along to its members discounts to a health fitness club that the members would be able to obtain directly from the health/fitness clubs.” August 14, 2002 Revisions, 67 Fed. Reg. 53186-7.

<sup>27</sup> “For example, a doctor that writes a prescription or refers an individual to a specialist for follow-up tests is engaging in a treatment communication and is not marketing a product or service.” August 14, 2002 Revisions, 67 Fed. Reg. 53186.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity<sup>28</sup>, 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.

*Payment* means:

(1) The activities undertaken by:

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

(ii) A health care provider<sup>29</sup> or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities,<sup>30</sup> obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

---

<sup>28</sup> Including a business associate. See August 14, 2002 Revisions, 67 Fed. Reg. 53187.

<sup>29</sup> Before the August 14, 2002 amendment, Paragraph (1)(ii) referred to "covered health care provider".

<sup>30</sup> "This allows reporting not just of missed payments and overdue debt but also of subsequent positive payment experience (e.g., to expunge the debt). We consider such positive payment experience to be "related to" collection of premiums or reimbursement." (December 28, 2000, Preamble, page 82495)

(F) Name and address of the health care provider and/or health plan.

\* \* \*

### § 164.502 Uses and disclosures of protected health information: general rules.

\* \* \*

(e) (1) *Standard: Disclosures to business associates.*

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information.<sup>31</sup>

(ii) This standard does not apply:

\* \* \*

(B) With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) apply and are met; or

(C) With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

\* \* \*

### § 164.504 Uses and disclosures: Organizational requirements.

\* \* \*

(a) *Definitions.*<sup>32</sup> As used in this section:

<sup>31</sup> “By law, the Privacy Rule applies only to health plans, health care clearinghouses, and certain health care providers. In today’s health care system, however, most health care providers and health plans do not carry out all of their health care activities and functions by themselves; they require assistance from a variety of contractors and other businesses. In allowing providers and plans to give protected health information (PHI) to these “business associates,” the Privacy Rule conditions such disclosures on the provider or plan obtaining, typically by contract, satisfactory assurances that the business associate will use the information only for the purposes for which they were engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with the covered entity’s duties to provide individuals with access to health information about them and a history of certain disclosures (e.g., if the business associate maintains the only copy of information, it must promise to cooperate with the covered entity to provide individuals access to information upon request). PHI may be disclosed to a business associate *only* to help the providers and plans carry out their health care functions – not for independent use by the business associate.” *Initial DHHS Guidance, July 6, 2001*

<sup>32</sup> The definitions of the following terms were removed and added to 45 CFR 164.103 at 68 FR 8334, 8381: Common control, Common ownership, Health care component, and Hybrid entity.

*Plan administration functions* means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

*Summary health information* means information, that may be individually identifiable health information, and:

- (1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and
- (2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

\* \* \*

(f) (1) *Standard: Requirements for group health plans.*

(i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of :

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) *Implementation specifications: Requirements for plan documents.* The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

- (B) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
- (C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
- (D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
- (E) Make available protected health information in accordance with § 164.524;
- (F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;
- (G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;
- (H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;
- (I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
- (J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

- (A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;
- (B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and
- (C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) *Implementation specifications: Uses and disclosures.* A group health plan may:

- (i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

- (ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;
- (iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and
- (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

### § 164.508 Uses and disclosures for which an authorization is required.

#### (a) Standard: authorizations for uses and disclosures.

(1) Authorization required: general rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.<sup>33</sup>

\* \* \*

#### (b) Implementation specifications: general requirements.

\* \* \*

(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document<sup>34</sup> to create a compound authorization, except as follows:

\* \* \*

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations.

(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except<sup>35</sup>:

<sup>33</sup> “[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.” August 14, 2002 Revisions, 67 Fed. Reg. 53220.

<sup>34</sup> “[S]uch as a notice of privacy practices or a written voluntary consent.” August 14, 2002 Revisions, 67 Fed. Reg. 53221.

<sup>35</sup> “[T]he Department eliminates the exception to the prohibition on conditioning payment of a claim on obtaining an authorization. Although some insurers urged that this conditioning authority be retained to provide them with more collection options, the Department believes this authorization is no longer necessary because we are adding a new provision in § 164.506 that permits covered entities to disclose protected health information for the payment purposes of another covered entity or health care provider. Therefore, that exception has been eliminated.” August 14, 2002 Revisions, 67 Fed. Reg. 53221.

\* \* \*

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

\* \* \*

(5) Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

\* \* \*

(c) Implementation specifications: Core elements and requirements.

\* \* \*

(2) Required statements. In addition to the core elements,<sup>36</sup> the authorization must contain statements adequate to place the individual on notice of all of the following:

\* \* \*

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

\* \* \*

<sup>36</sup> "Although the notification statements are not included in the paragraph on core elements an authorization is not valid unless it contains both the required core elements, and all of the required statements. This is the minimum information the Department believes is needed to ensure individuals are fully informed of their rights with respect to an authorization and to understand the consequences of authorizing the use or disclosure." August 14, 2002 Revisions, 67 Fed. Reg. 53221.

**§ 164.514 Other requirements relating to uses and disclosures of protected health information.**

\* \* \*

(g) *Standard: Uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such protected health information for any other purpose, except as may be required by law.

**§ 164.520 Notice of privacy practices for protected health information.<sup>37</sup>**

(a) Standard: notice of privacy practices<sup>38</sup>.

(1) Right to notice. Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice<sup>39</sup> of the uses and disclosures of protected health information that may be made by the covered entity<sup>40</sup>, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Exception for group health plans.

(i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO<sup>41</sup>; or

---

<sup>37</sup> Last updated December 8, 2002.

<sup>38</sup> **"Practices" defined:** "In this section of the final rule, we also refer to the covered entity's privacy "practices," rather than its "policies and procedures." The purpose of this change in vocabulary is to clarify that a covered entity's "policies and procedures" is a detailed documentation of all of the entity's privacy practices as required under this rule, not just those described in the notice. For example, we require covered entities to have policies and procedures implementing the requirements for "minimum necessary" uses and disclosures of protected health information, but these policies and procedures need not be reflected in the entity's notice. Similarly, we require covered entities to have policies and procedures for assuring individuals access to protected health information about them. While such policies and procedures will need to include documentation of the designated record sets subject to access, who is authorized to determine when information will be withheld from an individual, and similar details, the notice need only explain generally that individuals have the right to inspect and copy information about them, and tell individuals how to exercise that right." Preamble, page 82548.

<sup>39</sup> **Multiple notices:** "[C]overed entities may want or be required to produce more than one notice in order to satisfy the notice content requirements under this rule. For example, a covered entity that conducts business in multiple states with different laws regarding the uses and disclosures that the covered entity is permitted to make without authorization may be required to produce a different notice for each state. A covered entity that conducts business both as part of an organized health care arrangement or affiliated covered entity and as an independent enterprise (e.g., a physician who sees patients through an on-call arrangement with a hospital and through an independent private practice) may want to adopt different privacy practices with respect to each line of business; such a covered entity would be required to produce a different notice describing the practices for each line of business. Covered entities must produce notices that accurately describe the privacy practices that are relevant to the individuals receiving the notice." Preamble, page 82548.

<sup>40</sup> **Federal agencies:** "We note that all federal agencies must still comply with the Privacy Act of 1974. This means that federal agencies that are covered entities or have covered health care components must comply with the notice requirements of the Privacy Act as well as those included in this rule." Preamble, page 82548.

<sup>41</sup> **For example,** if a group health plan maintains both fully-insured and self-insured arrangements, the group health plan must, at a minimum, maintain and provide a notice that describes its privacy practices with respect to protected health information it creates or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

\* \* \*

(b) Implementation specifications: content of notice.<sup>42</sup>

(1) Required elements.<sup>43</sup> The covered entity must provide<sup>44</sup> a notice that is written in plain language<sup>45</sup> and that contains the elements required by this paragraph.

---

receives through the self-insured arrangements. This notice would be distributed to all participants in the self-insured arrangements (in accordance with § 164.520(c)(1)) and would also be available on request to other persons, including participants in the fully-insured arrangements." Preamble, pages 82547-8.

<sup>42</sup> **Notice requirements not exclusive:** "[T]he requirements for the content of the notice are not intended to be exclusive. As with the rest of the rule, we specify minimum requirements, not best practices. Covered entities may want to include more detail." Preamble, page 82548.

<sup>43</sup> **Layered notice:** "Covered entities may use a "layered" notice to implement the HIPAA Privacy Rule's requirements, so long as the elements required by 45 CFR 164.520(b) are included in the document that is provided to the individual. For example, a covered entity may satisfy the notice requirements by providing the individual with both a short notice that briefly summarizes the individual's 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. Providing the notice in this fashion is a helpful tool to assure that more individuals will realize that important information is contained in the notice." Guidance, December 4, 2002

<sup>44</sup> **Illiterates:** "We also encourage covered entities to be attentive to the needs of individuals who cannot read. For example, an employee of the covered entity could read the notice to individuals upon request or the notice could be incorporated into a video presentation that is played in the waiting area." Preamble, page 82549.

<sup>45</sup> **Meaning of "plain language":** "A covered entity can satisfy the plain language requirement if it makes a reasonable effort to: organize material to serve the needs of the reader; write short sentences in the active voice, using "you" and other pronouns; use common, everyday words in sentences; and divide material into short sections. We do not require particular formatting specifications ...." Preamble, page 82548-9.

**Non-English:** "[A]ny covered entity that is a recipient of federal financial assistance is generally obligated under Title VI of the Civil Rights Act of 1964 to provide material ordinarily distributed to the public in the primary languages of persons with limited English proficiency in the recipients' service areas. Specifically, this Title VI obligation provides that, where a significant number or proportion of the population eligible to be served or likely to be directly affected by a federally assisted program needs service or information in a language other than English in order to be effectively informed of or participate in the program, the recipient shall take reasonable steps, considering the scope of the program and the size and concentration of such population, to provide information in languages appropriate to such persons. For covered entities not subject to Title VI, the Title VI standards provide helpful guidance for effectively communicating the content of their notices to non-English speaking populations." Preamble, page 82549.

\* \* \*

(iii) Separate statements for certain uses or disclosures.<sup>46</sup> If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must<sup>47</sup> include a separate statement, as applicable, that:

\* \* \*

(C) A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

\* \* \*

(c) Implementation specifications: provision of notice. A covered entity must make the notice required by this section available on request to any person<sup>48</sup> and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) Specific requirements for health plans.

(i) A health plan must provide notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees; and

(C) Within 60 days of a material revision to the notice, to individuals then covered by the plan.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.<sup>49</sup>

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.<sup>50</sup>

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.<sup>51</sup>

<sup>46</sup> See section 164.502(i), which requires disclosures to be consistent with the notice.

<sup>47</sup> **Otherwise prohibited:** "If the covered entity does not include these statements in its notice, it is prohibited from using or disclosing protected health information for these activities without authorization." Preamble, page 82549.

<sup>48</sup> **Publicly available:** "The requestor does not have to be a current patient or enrollee. We intend the notice to be a public document that people can use in choosing between covered entities." Preamble, page 82551.

<sup>49</sup> **Distribution required only once:** "Unlike the proposed rule, we do not require health plans to distribute the notice every three years." Preamble, page 82551.

<sup>50</sup> **For example,** if an employee of a firm and her three dependents are all covered under a single health plan policy, that health plan can satisfy the initial distribution requirement by sending a single copy of the notice to the employee rather than sending four copies, each addressed to a different member of the family." Preamble, page 82551.

<sup>51</sup> **For example,** a health insurance issuer may have contracts with two different group health plans. One contract specifies that the issuer may use and disclose protected health information about the participants in the group health plan for research purposes without

\* \* \*

**§ 164.522 Rights to request privacy protection for protected health information.**

\* \* \*

**(b) (1) Standard: confidential communications requirements.**

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests<sup>52</sup> by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.<sup>53</sup>

(ii) A health plan must permit individuals to request and must accommodate reasonable requests<sup>54</sup> by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual,<sup>55</sup>

**(2) Implementation specifications: conditions on providing confidential communications.**

(i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

authorization (subject to the requirements of this rule) and one contract specifies that the issuer must always obtain authorizations for these uses and disclosures. The issuer accordingly develops two notices reflecting these different practices and satisfies its distribution requirements by providing the relevant notice to the relevant group health plan participants." Preamble, page 82551.

<sup>52</sup> **Standard for reasonableness:** "The reasonableness of a request made under this paragraph must be determined by a covered entity solely on the basis of the administrative difficulty of complying with the request and as otherwise provided in this section. A covered health care provider or health plan cannot refuse to accommodate a request based on its perception of the merits of the individual's reason for making the request." Preamble, page 82553.

**Examples:** "For example, the Department considers a request to receive mailings from the covered entity in a closed envelope rather than by postcard to be a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances. See 45 CFR 164.522(b)." OCR FAQ Answer ID 198 Updated 7/18/2003

<sup>53</sup> " **For example,** an individual who does not want his or her family members to know about a certain treatment may request that the provider communicate with the individual about that treatment at the individual's place of employment, by mail to a designated address, or by phone to a designated phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card, as an 'alternative means.'" Preamble, page 82553.

<sup>54</sup> **Standard for reasonableness:** "The reasonableness of a request made under this paragraph must be determined by a covered entity solely on the basis of the administrative difficulty of complying with the request and as otherwise provided in this section. A covered health care provider or health plan cannot refuse to accommodate a request based on its perception of the merits of the individual's reason for making the request." Preamble, page 82553.

<sup>55</sup> "**For example,** if an individual requests that a health plan send explanations of benefits about particular services to the individual's work rather than home address because the individual is concerned that a member of the individual's household (e.g., the named insured) might read the explanation of benefits and become abusive towards the individual, the health plan must accommodate the request." Preamble, page 82553.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

### § 164.530 Administrative requirements.

\* \* \*

(k) *Standard: group health plans.*<sup>56</sup>

(1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

---

<sup>56</sup> “Specifically, a group health plan that provides benefits solely through an issuer or HMO, and that does not create, receive or maintain protected health information other than summary health information or information regarding enrollment and disenrollment, is not subject to the requirements of this section regarding designation of a privacy official and contact person, workforce training, safeguards, complaints, mitigation, or policies and procedures. Such a group health plan is only subject to the requirements of this section regarding documentation with respect to its plan documents.” Preamble, pages 82563-4.

## V. Security Rule Requirements

### Sec. 164.314 Organizational requirements.

\* \* \*

- (b) (1) Standard: Requirements for group health plans.<sup>57</sup> Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to Sec. 164.504(f)(1)(ii) or (iii), or as authorized under Sec. 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
- (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to--
- (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;
  - (ii) Ensure that the adequate separation required by Sec. 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;
  - (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
  - (iv) Report to the group health plan any security incident of which it becomes aware.

---

<sup>57</sup> Compare to 45 CFR §164.504(f).

## VI. Comparison of Provider and Health Plan Policies

- MM** *Major modifications*  
**M** *Modifications*  
**SR** *Same regulatory issues, different details*  
**S** *Same or substantially similar*  
**N** *None required or not applicable*

Note: Whether and to what extent healthcare provider policies must be modified for health plan depends on the amount of specificity in the original and the amount desired in the health plan policies.

### I. No use or disclosure unless permitted

#### A. The “Basic Rule”

- M** 1. Confidentiality requirement  
 2. Definitional Issues
- SR** a. Designated records sets  
*Policy* [Original Policy](#)
- S** b. Definitions  
*Policy* [Original Policy](#)

#### B. Specific Disclosure Issues

- SR** 1. Organizational Issues  
 a. Hybrids and healthcare components  
*Policy*
- S** b. Affiliates  
*Policy* [Original policy](#)
- M** c. Organized health care arrangements  
*Policy*
- S** d. Business associate contracts  
*Policy* [Priv I.B.1.d.1](#)  
*Contract form* [Priv I.B.1.d.2](#)  
*Contract checklist* [Priv I.B.1.d.3](#)
- S** i. Brokers and agents  
*Policy*
- S** e. Group health plans  
*Policy*
- S** 2. Disclosure Issues  
 a. De-identification  
*Policy*
- S** b. Limited data set

	<i>Policy</i>	
	<i>Limited data set use agreement</i>	
SR	c. Minimum necessary - General	
	<i>Policy</i>	<a href="#">Priv I.B.2.c</a>
SR	Requests for non-routine disclosures	
	<i>Policy</i>	
S	d. Personal representative	
	<i>Policy</i>	Original Policy
S	e. Deceased individuals	
	<i>Policy</i>	

## II. Permitted uses & disclosures

---

### A. For treatment, payment and healthcare operations

	<i>Policy</i>	
	Consent ... and Acknowledgement	<a href="#">See below</a>
N	Treatment	
	<i>Policy</i>	Original policy
SR	Payment	
	<i>Policy</i>	Original policy
MM	Healthcare operations	
	<i>Policy</i>	Original policy
S	Health plan TPO	
	<i>Policy</i>	Original policy
SR	Sharing for other CE TPO	
	<i>Policy</i>	

### B. With authorizations - general

S	<i>Policy</i>	<a href="#">Original policy</a>
	Sample form (2 page)	<a href="#">Original form</a>
	Sample form (1 page)	<a href="#">Priv.II.B.3</a>
	Checklist	<a href="#">Original checklist</a>
MM	Marketing	
	<i>Policy</i>	
S	Psychotherapy notes	
	<i>Policy</i>	<a href="#">Original policy</a>

### C. "Opt-outs"

	<i>Policy</i>	
N	Facility Directories	
	<i>Policy</i>	<a href="#">Priv.II.C.1</a>
N	Patient alias	
	<i>Policy</i>	

N	Media policy <i>Policy</i>	
N	Disclosures to clergy <i>Policy</i>	
	Clergy disclosure designation form	
	Clergy designee approval letter	
M	Involvement in the Individual's care and notification purposes <i>Policy</i>	<a href="#">Priv.II.C.2</a>
N	Provision of notice in emergencies <i>Policy</i>	
<b>D. Exceptions</b>		
	<i>Policy</i>	<a href="#">Priv.II.D</a>
SR	1. required by law <i>Policy</i>	<a href="#">Original Policy</a>
N	2. public health activities - general <i>Policy</i>	<a href="#">Original Policy</a>
N	Child abuse reporting <i>Policy (Louisiana only)</i>	<a href="#">Original policy</a>
N	3. victims of abuse, neglect or domestic violence - general <i>Policy</i>	<a href="#">Original Polciy</a>
N	Adult abuse reporting <i>Policy (Louisiana only)</i>	<a href="#">Original Policy</a>
M	4. health oversight activities <i>Policy</i>	<a href="#">Original Policy</a>
SR	5. judicial and administrative proceedings <i>Policy</i>	<a href="#">Original Policy</a>
SR	6. law enforcement purposes <i>Policy</i>	
S	7. decedents <i>Policy</i>	
N	8. organ, eye, tissue donation <i>Policy</i>	
N	9. research purposes <i>Policy</i>	
	Research data use agreement	
	Research data use agreement - decedents	
	Research authorization form	
N	10. to avert serious threat to health or safety <i>Policy</i>	
N	11. specialized government functions <i>Policy</i>	

MM	12. worker's compensation <i>Policy</i>	<a href="#">Priv.II.D.12</a>
N	13. marketing <i>Policy</i>	
N	14. fundraising <i>Policy</i>	
S	15. underwriting <i>Policy</i>	
S	16. Whistleblowers and workforce member crime victims <i>Policy</i>	

### III. Other Patient Rights

#### A. Notice of privacy protections (§520)

M	<i>Policy</i>	<a href="#">Priv.III.A.1</a>
	Provision of notice in emergencies	
M	Notice form	<a href="#">Priv.III.A.2</a>
	Joint Notice	<a href="#">Priv.III.A.3</a>
N	Consent ... and Acknowledgement ...	<a href="#">Priv.III.A.4</a>
	Consent/Ack w/ involved persons	<a href="#">Priv.II.A.6</a>
M	Joint consent	<a href="#">Priv.II.A.7</a>

#### B. Privacy Requests (§522)

SR	1. Request for restriction <i>Policy</i>	<a href="#">Priv.III.B.1</a>
	Request for additional restrictions form	<a href="#">Priv.III.B.1.a</a>
	Subject to an agreed upon restriction <i>Policy</i>	
SR	2. Request for alternative communication <i>Policy</i>	<a href="#">Priv.III.B.2</a>
	Request for alternative communication form	<a href="#">Priv.III.B.1.a</a>

#### C. Access - inspection and copying (§524)

SR	<i>Policy</i>	<a href="#">PRIV.III.C.1</a>
	<i>Reviewable denial letter</i>	
	<i>unreviewable denial letter</i>	

#### D. Amendment (§526) - General

SR	<i>Policy</i>	<a href="#">Priv.III.D.1</a>
	<i>Suspension of right</i>	
	<i>Denial letter</i>	<a href="#">Priv.III.D.2</a>
	<i>Request Form</i>	<a href="#">Priv.III.D.3</a>
	<i>Amendment process flow-chart</i>	

#### E. Accounting for disclosures (§528)

M

*Policy* [Priv.III.E.1](#)  
*Request*  
*Disclosure accounting*  
*Suspension log*

## IV. Administrative Requirements

	<i>Policy</i>	<a href="#">Priv.IV</a>
	<b>A. personnel designations</b>	
	<i>Policy</i>	
SR	1. Privacy Officer	
	<i>Policy</i>	<a href="#">Priv.IV.A</a>
SR	2. Other designations	
	<i>Policy</i>	
SR	<b>B. training</b>	
	<i>Policy</i>	<a href="#">Original Policy</a>
SR/M	<b>C. safeguards &amp; security</b>	
	<i>Policy</i>	<a href="#">Priv.IV.C</a>
	<i>Confidential communications</i>	
	<i>Display of patient information</i>	
	<i>Employee confidentiality statements</i>	
	<i>Non-workforce confidentiality statements</i>	
	<i>External agency representatives</i>	
	<i>Information confidentiality agreements</i>	
	<i>External representatives &amp; vendors</i>	
	<i>Storage of PHI</i>	
	<i>Disposal and destruction of PHI</i>	
	<i>Faxing information</i>	
SR	<b>D. complaints to the covered entity</b>	
	<i>Policy</i>	<a href="#">Priv.IV.D.</a>
SR	<b>E. sanctions</b>	
	<i>Policy</i>	<a href="#">Priv.IV.E</a>
S	<b>F. mitigation</b>	
	<i>Policy</i>	<a href="#">Priv.IV.F</a>
S	<b>G. non-retaliation</b>	
	<i>Policy</i>	<a href="#">Priv.IV.E</a>
S	<b>H. non-waiver</b>	
	<i>Policy</i>	<a href="#">Priv.IV</a>
S	<b>I. policies and procedures</b>	
	<i>Policy</i>	<a href="#">Priv.IV.I</a>
	Changes necessitated by changes in the law	
	<i>Policy</i>	

**S J. documentation**

*Policy*

Priv.IV.J

**S K. group health plans**

*Policy*

**SR L. verification**

*Policy*

Priv.IV.L

---

**V. Technical Provisions**

**S A. Preemption of State Law**

**S B. Compliance and Enforcement**

**S C. Transition Provisions**

## VII. Final Thoughts

### What is the HIPAA “firewall?”

A health plan and its sponsor may look the same to you, but, even though they often share employees, you must distinguish between them in order to build your “HIPAA firewall.”

Health Plan      Plan Sponsor/Employer

The HIPAA Privacy Rule requires the plan to document adequate separation between the plan and its sponsor by listing in the plan document those employees (by name or class) with access to PHI. This is part of the “firewall.”

### How should an employer build the “firewall” that it must build in order to receive PHI for administrative functions?

- evaluate which employees have access to PHI (example: the HR Director, the employees in the Benefits Department, accounting employees, IT employees, etc.)
- implement procedure to ensure: (a) that only the designated employees have access to PHI, and (b) that even the designated employees only have access to the minimum necessary amount
- describe the “firewall” procedures in the plan document

### What “firewall” procedures must be described in the plan document?

In order for there to be adequate separation between the group health plan and the plan sponsor (see 45 C.F.R. Part 164.504(f)(2)(iii)), the plan documents must provide:

- a description of those employees or class of employees or other persons under the control of the plan sponsor to be given access to PHI;
- restrictions on the access to and use by such employees of PHI for non-plan functions; and
- an effective mechanism for resolving any issues of noncompliance by the persons who are authorized above to receive PHI.

### What are some mistakes to avoid in HIPAA Privacy Rule implementation?

- issuing HIPAA Privacy Rule notices and policies in the name of the employer and not the plan (remember: the plan, not the employer is the covered entity – if you issue privacy notices and policies in the employer name, you are compromising the firewall that is supposed to separate the plan and the employer)
- promulgating boilerplate privacy policies and procedures, never really implementing them, and not really reading them very carefully until the night before you are deposed in a breach of privacy lawsuit
- failing to train new HR or benefit personnel about the Privacy Rule (the training obligation is on-going, so you might want to videotape your training session and show it to new hires)

- doing a slap-dash job of creating a plan document for your health plan (plan documents have IRS, ERISA and Sarbanes-Oxley implications and must be prepared or reviewed by experienced benefits counsel)
- failing to obtain board approval of your plan document (plan documents must be formally adopted by the board)
- promulgating a plan document that fails to indemnify the plan administrator (possibly you) and other benefits or HR personnel who may be exposed to personal liability for their service to the plan
- thinking that the general release in a job application or in a medical records release will protect an employer from liability under the HIPAA Privacy Rule – only a HIPAA Privacy Rule written authorization will do this
- thinking that you must buy “HIPAA compliant” file cabinets – any locked file cabinet should work fine