

## ChoiceNet/InterCare Health Plans Getting Your Arms Around HIPAA Compliance

The enclosed packet includes basic HIPAA Privacy Rule information, Amendments for your health care plan, identified action items and sample forms.

The Health Insurance Portability and Accountability Act (HIPAA) privacy rules go into effect for most employer group health plans by April 14, 2003. How the plans comply depends on the type of health care plan and what kind of health information they collect and maintain.

The following information is based on the HIPAA statute and the August 2002 final rules from the Department of Health and Human Services' Office of Civil Rights.

### **Basic Privacy Rules:**

- (1) If your organization uses or discloses protected, individually identifiable, health information, it will be compelled to comply in one or more ways with the HIPAA privacy rules.
- (2) The privacy rules technically apply to covered entities, which include health plans, health care clearinghouses, and health care providers who transmit any health care information electronically.  
Group health plans include medical, dental, and long-term health plans and health flexible spending accounts. Employee assistance programs (EAP's) that provide medical care services are also likely to be considered group health plans.

### **Questions to Consider:**

- (1) **Does the employer or plan sponsor (and not the group health plan itself) handle protected health information? PHI is individually identifiable health information that is transmitted or maintained in electronic or any other medium.** If the answer is yes, the use of the protected health information is governed by the privacy rules.
- (2) **Does the employer health plan have annual receipts of \$5 million or less?** If the answer is yes, the plan does not have to comply with the privacy rules until April 14, 2004, a year later than larger plans.
- (3) **Does the employer health care plan have fewer than 50 participants?** If the answer is yes, then the plan is not subject to the privacy rules. Note, however, that more restrictive state laws take precedence and small plans may be subject to privacy rules. It is a good idea to comply with the privacy rules regardless of the size of the plan. If the plan increases its membership rapidly, it may then be subject to the privacy rules and the procedures would already be in place.

- (4) **Is the employer health care plan fully insured?** If the answer is yes, HMOs and insurance companies in fully insured plans generally bear the burden of compliance with the privacy rules. The extent to which employers with insured plans may be subject to the privacy rules depends on their access to PHI.
- (5) **Is the employer health care plan self-funded and/or self-administered?** Self-funded and self-administered plans generally are subject to the privacy rules, because these plans need PHI to maintain the plan. Self-administered plans with fewer than 50 participants, which include some Sec. 125 flexible spending accounts, however, are exempt from the privacy rules.
- (6) **Does the health care plan use third parties for any type of administration in which PHI is used?** Health care plans must include certain contractual requirements in arrangements with their vendors and service providers (“business associates”) who handle PHI. This effectively requires that business associates maintain the privacy of medical information according to the HHS rules.
- (7) **Is the employer a hybrid entity?** “Hybrid entities” are covered entities that designate a separate health care component(s). Transfer of protected health information held by the health care component to other components of the hybrid entity continues to be a disclosure under the privacy rules. The final rules clarify that an employer is not a hybrid entity simply because it is the plan sponsor of a group health plan.

## **Protected Health Information**

The goal of the rules is to safeguard protected health information (PHI). If an employer uses or discloses PHI, it will have to comply with many of the privacy rules.

**PHI is individually identifiable health information that is transmitted or maintained in electronic or any other medium.** According to the 2002 final rules, PHI does not include employment records held by an employer nor certain education records in the Family Education Rights and Privacy Act. Psychotherapy notes are a special class of information that almost always will require an authorization for use and disclosure.

The final rules clarify that medical information needed for an employer to carry out its obligations under the Family and Medical Leave Act, the Americans with Disabilities Act, and similar laws, as well as records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees may be part of the employment records maintained by the covered entity in its role as an employer.

The privacy rule applies to individually identifiable health information in all forms, electronic, written, oral and any other.

Individually identifiable health information has several characteristics:

1. It relates to the physical or mental health of an individual; the provision of health care to an individual (including insurance processes, quality assessment, case management, and disease and disability management activities); or the payment for the provision of health care to an individual (including claims processing, utilization review, and coordination of benefits);
2. It is created or received by a health care provider, health plan, employer, or health care clearinghouse;
3. It identifies the individual, or there is a reasonable basis to believe the information can be used to identify the individual.

### De-Identifying Information

The final rules note that PHI can be “de-identified” and thus be exempt from the rules. Employers with insured health plans may not want health care information for cost analysis, claims analysis, contract renewals, or other purposes. Employers can be assured that the information has been de-identified in one of two ways:

1. A knowledgeable and experienced person determines that the risk is very small that the health information can be individually identified and that person documents how that determination was made; or
2. All of the identifiers of the individual or of relatives, employers, or household members of the individual are removed.

#### Items That must be removed To De-Identify PHI\*

Names	All geographic subdivisions**	All elements of dates (except year)***
Telephone numbers	Fax numbers	Electronic mail addresses
Social security numbers	Medical record numbers	Health plan beneficiary numbers
Account Numbers	Certificate/license numbers	Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers	Web Universal Resource Locators (URLs)	Internet Protocol (IP) address numbers
Biometric identifiers, including finger and voice prints	Full face photographic images and any comparable images	Any other unique identifying number, characteristic, or code

\* Additionally, the covered entity cannot have knowledge that the information could be used with other information to identify an individual.

\*\*Applies to subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes, except for the initial three digits of a zip code if:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

\*\*\*Applies to dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all

ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

## **Employer Use of PHI**

The employer's health plan, and not the employer, can have access to PHI related to treatment, payment, and health care operations (TPO). However, the employer itself may obtain PHI in to ways:

1. An employee may authorize *in writing* the disclosure of specific PHI to the employer.
2. If an employer wants access to PHI for plan administrative functions without authorization, it must amend the group health plan document to impose specified limits on the use and disclosure of the information. For example, use must be limited to plan purposes and access restricted to a specified group of individuals involved in plan administration. The employer will also be required to certify that the plan amendments have been made and that it agrees to follow the applicable restrictions.

Plan administrative functions include quality assurance, claims processing, auditing, and monitoring.

## **Amend Plan Document: Separate Plan, Sponsor**

Provide for adequate separation ("firewall") between the group health plan and the plan sponsor by including in the plan document the following:

- A. Describe those employees to be given access to protected health information from the plan;
- B. Restrict the access to and use by such employees 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 these employees.

Additionally, summary information may be provided to the employer. For purposes of obtaining premium bids or amending or terminating a group health plan, an insurer, HMO, or other health plan may disclose summary health information (which has been de-identified except for five digit zip codes). Transfer of protected health information held by the health care component to other components of the hybrid entity continues to be a disclosure under the privacy rules.

The final rules continue the exemption concerning disclosures of enrollment information to health plan sponsors. Thus, health plans (including health insurers and HMOs) are permitted to disclose enrollment or disenrollment information to a plan sponsor without meeting the plan document amendment and other related privacy requirements.

## **Hybrid Entities**

Because only the health care component part of a “hybrid entity” must be HIPAA compliant, employers that are “Hybrid entities” must make sure that PHI stays within the health care component of the employer. (Hybrid Entity: A covered entity whose covered functions (under HIPAA) are not its primary functions.)

Any use or disclosure of PHI by the health care component of the hybrid entity is subject to the privacy standards even when such issue or disclosure is made internally within the hybrid entity. Moreover, the health care components of hybrid entities are required to implement firewalls or safeguards between itself and the larger hybrid entity in order to insure meaningful privacy protection.

Hybrid entities must comply with the HIPAA privacy regulations. However, the privacy regulations apply only to the part of the entity that is the health care component. If, for example, in a factory with a clinic, the business office handles both health clinic records and the company’s personnel records, the business office would be required to protect only the clinic records, not the personnel records.

Hybrid entities must erect firewalls to protect against the improper use or disclosure within or by the organization. In the example above, the company would need to establish firewalls with respect to the records systems to ensure the clinic records were handled in accordance with the HIPAA privacy rules.

The final rules clarify that an employer is not a hybrid entity simply because it is the plan sponsor of a group health plan. The employer/plan sponsor and group health plan are separate legal entities and, therefore, do not qualify as a hybrid entity.

Many employers will be surprised to find, however, that HIPAA considers them to be hybrid entities, such as the following:

1. A factory or manufacturer, which maintains an employee health clinic and transmits any protected information in electronic form.
2. A government department that provides health services.
3. A company that owns a large national chain of outpatient and residential mental health facilities.
4. A school system with school nurses or other licensed health professionals, which transmit any protected health information in electronic form.
5. A health center at a college or university which transmits protected health information electronically in connection with claim requests.

In each of these examples, the non-health care related activities of the organization should be walled off from the “health care component” of the organization (which involves the HIPAA-covered activities).