



Z.A.G/S&W

HIPAA Privacy Requirements

The federal law known as HIPAA -- the Health Insurance Portability and Accountability Act -- included a Congressional mandate designed to protect the privacy of an individual's health care information. When Congress failed to adopt a health care privacy law, the task fell to the Department of Health and Human Services, which has been working on regulations since 1999. DHHS has now issued final regulations that establish a uniform set of federal privacy rules. The effect of those regulations on employers sponsoring health plans is summarized in this advisory.

The new privacy rules became applicable April 14, 2003, although small health plans (generally plans with less than \$5 million of premiums or claims paid during the last full fiscal year) have until April 14, 2004 to comply. A fully insured health plan that does not receive so-called protected health information does not have to comply with the majority of the new rules. A self-insured and self-administered health plan with fewer than fifty participants also does not have to comply with the rules. Fully insured health plans that receive protected health information and self-insured health plans, including health flexible spending accounts, are, unless otherwise excepted, subject to full compliance with the new rules.

BOSTON

NEW YORK

TEL-AVIV

WASHINGTON, DC

www.zag-sw.com

Table of Contents

Some Key Definitions..... 2

Using Protected Health Information..... 3

Day-to-Day Operations 5

Administrative and Firewall Requirements 6

Individual Rights and Disclosures..... 7

Failure to Comply 8

HIPAA Preemption of State Law 8

Other HIPAA requirements..... 8

Appendix A

Appendix B

Appendix C

Some Key Definitions

The new privacy rules impose three sets of privacy-related obligations on covered entities: limitations on the use and disclosure of protected health information; administrative requirements for compliance; and individual rights. The privacy rules generally regulate how and when covered entities may use and disclose protected health information. Before exploring the effect of each of these obligations on an employer, some new jargon must be introduced.

Covered Entities. Covered entities are: health plans; health care providers (such as physicians, pharmacies, and nursing homes) that conduct certain transactions electronically; and health care clearinghouses. Although an employer is not a covered entity, in many cases the employer is affected by the new privacy rules because it receives protected health information from the health plan(s) it sponsors.¹

Health Plan. A health plan for these purposes is any plan that on an individual or group basis provides (or pays the cost of) medical care. Health insurers, HMOs and issuers of long-term care policies are health plans, as are welfare benefit plans subject to ERISA. Thus, the term health plan can include:

- limited scope dental and vision plans;
- health flexible spending accounts (or health FSAs);
- prescription plans; and
- certain employee assistance programs and on-site clinics.

A health plan does not include an arrangement that does not offer medical care, such as a plan offering:

- life insurance;
- workers' compensation;
- accident only or disability insurance; and
- liability insurance.

The definition of health plan for these purposes also excludes a self-insured, self-administered plan that has fewer than fifty participants. As a practical matter, however, this exception may only be of value in the health FSA context, since most small employers do not find self-insured health plans to be economically attractive.

Health Information. Health information is any information, in any form, that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care for an individual. Health information can be created or received by a wide variety of entities including health plans, life insurers, health care providers, employers and schools and universities.

Protected Health Information. Protected health information (or "PHI") is individually identifiable health information that is transmitted or maintained electronically or in any other form (oral, written, etc.). Individually identifiable health information is health information that identifies (directly or indirectly) the individual to which it relates and is created or received by a health care provider, a health plan, an employer or a health care clearinghouse. Thus, an employer may create PHI, but unless the employer is a covered entity, use or disclosure of the PHI is not regulated by these new rules.²

¹ This advisory assumes that the employer is not otherwise involved in the health care industry, which could cause it to be a covered entity in its own right.

² An example illustrates the complexity of these new rules. Suppose an employer requires a drug test as a condition of employment. If the test is administered by an independent blood lab, which appears not to be a

Individually identifiable health information that is de-identified (discussed further below) is not treated as PHI subject to the privacy rules.

Using Protected Health Information

PHI may be used or disclosed³:

- to the individual;
- for treatment, payment or health care operations;
- as permitted or required by HIPAA (governmental purposes such as use by DHHS in a compliance audit or in connection with the enforcement of the rules);
- pursuant to an authorization; or
- in certain circumstances, as disclosed to and agreed to by that individual in advance.⁴

A covered entity must make reasonable efforts to limit any use or disclosure of PHI to the *minimum necessary* to accomplish the intended purpose. The minimum necessary standard does not apply to disclosure to or by a health care provider for treatment or to disclosures pursuant to an authorization.

Disclosure of PHI to employer/health plan sponsor. There is no blanket exception that permits the disclosure of PHI to the employer/health plan sponsor of the individual (whether for use in an employment-related or other benefit matter). In fact, an employer's access to individually identifiable health information is quite limited under the new privacy rules. If the employer seeks to avoid the privacy rules, the employer may only receive the following:

- Summary health information if requested in order to obtain bids for coverage or in connection with the modification, amendment or termination of a health plan;
- disclosure concerning whether an individual is participating in a health plan or is enrolled with or disenrolled from a health insurance issuer or HMO (but not necessarily any other information, such as whether a preexisting condition limitation might apply); and
- PHI pursuant to an authorization.⁵

If, on the other hand, the employer is willing to comply with the privacy rules (or effectively is forced to comply in the case of a self-insured plan), it may receive PHI in connection with plan administrative functions once it certifies that it has amended the health plan as necessary to comply with the privacy rules and has established appropriate firewalls (as described below).

For other employers, disclosure pursuant to an authorization will be particularly important, such as when an employer desires to intervene on behalf of a health plan participant in connection with a coverage dispute. While the health plan participant is always free to disclose what might be considered PHI to an employer, the employer may find that an insurer is unwilling to discuss a

covered entity, the result of the test, which is PHI, may be disclosed to the employer and used by the employer without regard to these rules. Suppose instead the test is administered at a hospital – a health care provider and a covered entity. The result of the test generally cannot be disclosed by the hospital directly to the employer. The solution to this problem is to obtain a disclosure authorization from the individual, and receipt of such an authorization can be a condition of employment. Authorizations are discussed more fully below.

³ Under the regulations, "use" refers to a covered entity's internal utilization of PHI. "Disclosure" refers to the communication of PHI to any party outside the covered entity. Thus, a health plan may "use" PHI in evaluating a claim but may not "disclose" that PHI to, for example, the employer's disability carrier except to the extent the privacy rules are satisfied.

⁴ This could include, for example, disclosure to family members for health care purposes. The new rules also permit the designation of a personal representative to act on behalf of an individual, and parents can usually represent a minor child.

⁵ In the first two situations, individuals must also be informed of the disclosure in the privacy notice (discussed below).

participant's situation with the employer without an authorization from the participant since any meaningful benefit discussion may of necessity require disclosure of PHI by the insurer to the employer. Further, disclosure pursuant to an authorization may be the only way PHI obtained by a health plan or health care provider can be disclosed to an employer who is processing a request for an accommodation under the Americans with Disabilities Act or is evaluating an employee's FMLA leave request due to a serious health condition. Finally, a health plan may condition enrollment on execution of an authorization designed to facilitate enrollment.

What is a valid authorization? For an authorization to be valid, it must be written in plain language, signed and dated by the individual, and contain:

- a fairly specific description of the information to be used or disclosed (although one could permit disclosure of a person's entire medical record by authorizing disclosure of "all health information");
- the identity of the person(s) authorized to make the requested use or disclosure as well as the identity of the recipient of the information (a long-term disability insurer, for example);
- a description of the purpose of the requested use or disclosure; and
- an expiration date or event.

In addition, the authorization must contain the following notices:

- right to revoke the authorization at any time pursuant to a written revocation, including appropriate instructions;
- explanation of the ability or inability of the health plan to condition treatment, payment, enrollment or eligibility for benefits on the authorization; and
- a statement that the PHI disclosed pursuant to the authorization might be subject to redisclosure by the recipient and no longer protected by HIPAA (such as when health information is disclosed to a disability insurer).

Authorizations (for various purposes or for various potential recipients) may be combined, but an authorization cannot be combined with another type of document, such as a patient consent form. The covered entity must provide a copy of the authorization to the individual and document and retain the authorization for six years. Note, however, that the covered entity need not maintain records of disclosure pursuant to the authorization.

Situations where an authorization is not required. An authorization is not required prior to disclosure of PHI in about twelve public policy situations, such as disclosures for law enforcement purposes or for compliance with workers' compensation laws. The regulations specify conditions on disclosure under several of the exceptions and, for the most part, any disclosure must still satisfy the minimum necessary standard.

PHI that is "de-identified" is not subject to restrictions on its use or disclosure. De-identified health information is health information that does not permit the identification of the individual to whom it relates. The regulations specify eighteen data items (such as name, phone number, account number, etc.) that must be deleted from the record in order to de-identify the information.

As indicated earlier, an employer may also receive summary health information, which is PHI that has been de-identified and summarized (by claims history, expenses, etc.). Summary health information may be used, for example, when comparing potential insurance providers. If the employer intends to receive summary health information, the privacy notice must so state.

Examples of the new rules in operation.

Health FSA: An employee wants to pay her dentist with funds from her health FSA. The dentist may disclose PHI for its own payment purposes. Therefore, the dentist may send the bill, which will be as terse as possible in order to satisfy the minimum necessary standard, directly to the health FSA for payment, even if the health FSA is not a covered entity. However, if the employee pays the bill and seeks reimbursement from the health FSA, the

dentist cannot disclose PHI directly to the health FSA without a valid authorization, unless the health FSA is a covered entity. Assuming the health FSA is a covered entity, the dentist may disclose PHI directly to the health FSA.

FMLA: Employers often obtain medical certifications to verify that an employee has a "serious health condition" under the FMLA. As a result of these new rules, an employer will need to obtain a valid authorization before a covered entity can provide the certification. Accordingly, existing FMLA policies may need to be reviewed and perhaps amended for compliance with the new HIPAA privacy rules.

Workers' Compensation: An employee is injured at work and applies for workers' compensation benefits. To determine if the employee is eligible for benefits, the employer may need information from a covered entity regarding the medical condition of the employee. The employer cannot generally obtain information on the employee's medical condition without a valid authorization. There is, however, an exception in the regulations for disclosures when legally required under state workers' compensation laws. Therefore, if applicable state law requires that the covered entity disclose the information to the employer, an authorization will not be required.

Day-to-Day Operations

HIPAA permits a covered entity to disclose PHI to a "business associate" that is hired to perform related functions if certain requirements are met. Specifically, business associates must generally agree to abide by the same HIPAA disclosure restrictions imposed on the covered entity that provides the PHI.

A business associate is an entity or person who:

- performs or assists in performing a function or activity involving the use or disclosure of PHI or any other function or activity regulated by HIPAA (including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation or financial services and has access to PHI.

Thus, a third-party administrator of a self-insured health plan is a business associate with respect to the health plan, as is outside counsel engaged in representing the health plan in, for example, a benefit claim.⁶ The term business associate, however, does not include employees of a covered entity (in the case of, for example, a self-insured health plan) and those working under the covered entity's direct control.

The privacy obligations of a business associate must be set forth in a contract. (Note, however, that a health plan does not need a business associate contract with the insurer if the health plan is fully insured.) A business associate contract must:

- establish the permitted and required uses and disclosures of PHI, which may not exceed the uses and disclosures allowed for the covered entity;
- prohibit the business associate from using or disclosing the information other than as permitted by the contract or by law;
- require the business associate to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the contract or by law;

⁶ Other examples of business associates include the health plan's broker, a third-party engaged in assisting the health plan with COBRA administration or health FSA administration, and (possibly) the employer's payroll vendor.

- require the business associate to report to the covered entity any improper use or disclosure of PHI;
- require the business associate to ensure that any of its agents or subcontractors agree to the same restrictions that apply to the business associate;
- require the business associate to provide individuals with access to their PHI;
- require the business associate to make available its internal books and records to DHHS for purposes of determining the covered entity's compliance with HIPAA;
- require the business associate to return or destroy all information at the termination of the contract and retain no copies or, if not feasible, to extend the protections set forth in the contract; and
- permit termination if there is a material violation of a term of the contract.

The deadline for entering into new business associate contracts that satisfy the regulations is generally April 14, 2003, but small plans have until April 14, 2004. Additionally, certain plans that had business associate contracts in place as of October 15, 2002 have until the earlier of (i) the date the business associate contract is amended or (ii) April 14, 2004 to update their contracts. Once the deadline passes, a covered entity cannot provide PHI to a business associate unless an appropriate business associate contract is in effect.

And, as should be expected, simply executing a business associate contract is not enough. Under ERISA on-going monitoring is necessary to ensure compliance with the privacy rules by the business associate.

Administrative and Firewall Requirements

Employers that will receive PHI from a fully insured health plan and employers acting as the administrator of a self-insured health plan must satisfy various administrative and firewall requirements with respect to PHI.

Plan documents. PHI may be disclosed by a covered entity to an employer only after health plan documents are amended to provide for the use and protection of PHI. Specifically, health plan documents must be amended to reflect the employer's agreement:

- not to use or further disclose PHI other than as permitted or required by the plan documents or as required by law;
- to ensure that any agents and subcontractors to whom it provides PHI received from the health plan agree to the same restrictions and conditions that apply to the plan sponsor;
- not to use or disclose PHI for employment related actions and decisions or in connection with any other benefit or employee benefit plan;
- to report to the health plan any use or disclosure of PHI that is inconsistent with permitted uses or disclosures;
- to make available PHI to individuals, including for amendment and accounting purposes;
- to return or destroy all PHI received from the health plan and to retain no copies when no longer needed or, if not feasible, to limit use of such PHI; and
- to make its internal practices, books, and records relating to the use and disclosure of PHI available to DHHS for purposes of determining compliance with HIPAA.

Firewall and other procedural safeguards. The employer must also create a "firewall" designed to limit access to PHI and to provide adequate separation between the health plan and the employer. This includes describing in the plan documents the employees (or classes of employees) that may be given PHI, restricting the access to and use of PHI by such employees, and providing an effective mechanism for resolving issues of noncompliance.

In addition, the employer needs to: appoint a privacy official who is responsible for the development and implementation of the policies and procedures; designate a contact person who is responsible for receiving complaints and who is able to provide further information about matters covered in the privacy notice (this can be the same person as the privacy official); train all existing

and new employees on the new policies and procedures; establish technical safeguards (such as computer firewalls) and physical safeguards (such as locking cabinets) to protect the PHI; provide a process for individuals to make complaints and document all complaints; create and apply a system to enforce sanctions on members of the workforce who do not comply with the privacy policies and procedures; and mitigate any harmful effects (to the extent practicable) of a use or disclosure of PHI.

Finally, the employer may not take adverse action against individuals exercising their rights, filing a complaint, testifying, assisting or participating in an investigation or opposing any improper practice under HIPAA, nor may the employer require an individual to waive his rights under HIPAA.⁷

Individual Rights and Disclosures

The new privacy rules create the following individual rights:

- right to receive a privacy notice;
- right to access, including the right to copy, the individual's own PHI;
- right to amend the individual's own PHI; and
- right to an accounting of disclosures of PHI.

All health plans must provide a written privacy notice to individuals enrolled in the health plan. A fully insured plan that does not receive PHI does not have to provide a privacy notice – the obligation is on the insurer. A fully insured plan that receives PHI (other than summary health and enrollment information) must maintain a privacy notice, but only has to provide it upon request – again, the primary obligation to provide the notice is on the insurer.

The notice must be in the format of and contain information specified in the privacy regulations (generally a description of the uses and disclosures of PHI that may be made by the covered entity, the individual's rights and the legal obligations of the covered entity with respect to PHI) and must be provided to all employees enrolled in the plan (a single notice to the named insured or covered employee is sufficient for all covered dependents). The notice must be provided by the compliance date (April 14, 2003 for large plans and April 14, 2004 for small plans). Additionally, the notice must be provided to each individual upon enrollment in the health plan and within sixty days of any material revision to the notice. Furthermore, at least every three years, the health plan must notify individuals of the availability of this notice.⁸ In a slight set-back to the electronic delivery movement, the regulations provide that the notice may be provided by e-mail only if the recipient agrees to receive the notice electronically.⁹

As noted, an individual has the right to access and copy his or her PHI. This right, which is imposed on any covered entity, presumably is most relevant to health care providers although the obligation may at times affect a health plan. A covered entity generally must respond to a request within thirty days of the request if the information is on site or within sixty days (generally) if the information is off site. If a covered entity does not have the information but knows where it is, the covered entity is obligated to tell the individual where to direct his request for the information. Access may be denied in certain circumstances and the covered entity may require that an individual make an access request in writing. Additionally, the individual may be charged for copies and other costs.

⁷ Although a fully insured plan that does not receive protected health information is not generally subject to the administrative and firewall requirements, an employer sponsoring a fully insured plan cannot retaliate against an individual who exercises his rights under HIPAA and cannot require an individual to waive his rights under HIPAA.

⁸ The notice may, but need not, be part of an SPD.

⁹ The notice must also be posted on a covered entity's website if the covered entity maintains a website with information about the covered entity's customer service or benefits.

An individual may ask that PHI that is inaccurate or incomplete be amended. The covered entity must respond within sixty days of the request, which time may be extended for another thirty days. A covered entity must establish a procedure to track and timely respond to such requests.

Finally, an individual has the right to receive an accounting of disclosures of his or her PHI other than disclosure related to treatment, payment, or health care operations, and certain other disclosures. The accounting must specify the nature of the disclosure, the identity of the recipient and an explanation of the purpose for the disclosure. A request for an accounting must generally be responded to within sixty days.

Failure to Comply

Failure to comply with the new privacy rules may result in a civil penalty of up to \$100 per day per violation (not to exceed \$25,000 per violation per calendar year). Criminal penalties may also apply if a person knowingly misuses PHI.

Although HIPAA does not permit individuals to pursue a private course of action in the event of a violation of the new privacy rules, complaints may be lodged with the DHHS's Office for Civil Rights. HIPAA also provides that a covered entity may not retaliate against an employee, participant or other individual filing a complaint. State law causes of action are not barred, nor are causes of action that may be available under ERISA.

HIPAA Preemption of State Law

The idea behind the HIPAA privacy rules was to create a uniform set of privacy obligations. Accordingly, state privacy laws relating to health care are generally preempted to the extent the state law is contrary to HIPAA. State law survives, however, when: (1) state law is more stringent; (2) state law regulates certain reporting requirements (such as the reporting of child abuse); (3) DHHS determines that a particular provision of state law is necessary (such as laws designed to prevent fraud and abuse or to ensure appropriate state regulation of insurance); and (4) state laws relate to the licensing and monitoring of health plans.

Other HIPAA Requirements

In addition to the new privacy rules, HIPAA imposes new security standards, designed to protect individually identifiable health information. The standards require appropriate administrative, technical, and physical safeguards. Security regulations were finalized February 20, 2003 and become applicable on April 21, 2005.

HIPAA also implements new electronic transaction standards, designed to promote electronic data interchange. These rules are generally effective October 16, 2003.

The security and electronic standards, like the privacy rules themselves, affect health plans and will be of greatest concern to employers who maintain self-insured health plans.

David Guadagnoli, Esq.
Pamela Fleming, Esq.
ZAG/S&W LLP
One Post Office Square
Boston, MA 02109
617 338 2800

© 2003 Zysman Aharoni Gayer & Co./Sullivan & Worcester LLP

Because sound legal advice must necessarily take into account all relevant facts and developments in the law, the information you will find in this Advisory is not intended to constitute legal advice or a legal opinion as to any particular matter.

APPENDIX A

To Do List for Employers

Step 1: Make a list of all your welfare benefit plans offering medical or other health benefits, including health FSAs, dental plans, etc. There is a decision tool to help you identify health plans at:

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

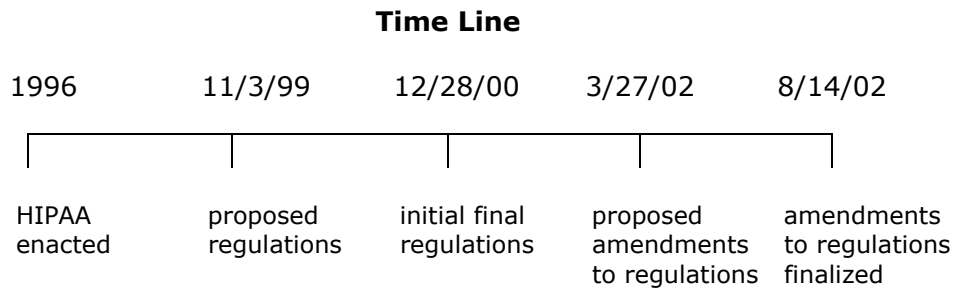
Step 2: Identify which health plans are self-funded and which health plans are fully insured

Step 3: Determine which of the fully insured health plans will receive PHI

Step 4: Follow flowchart at Appendix B to determine the level of compliance required

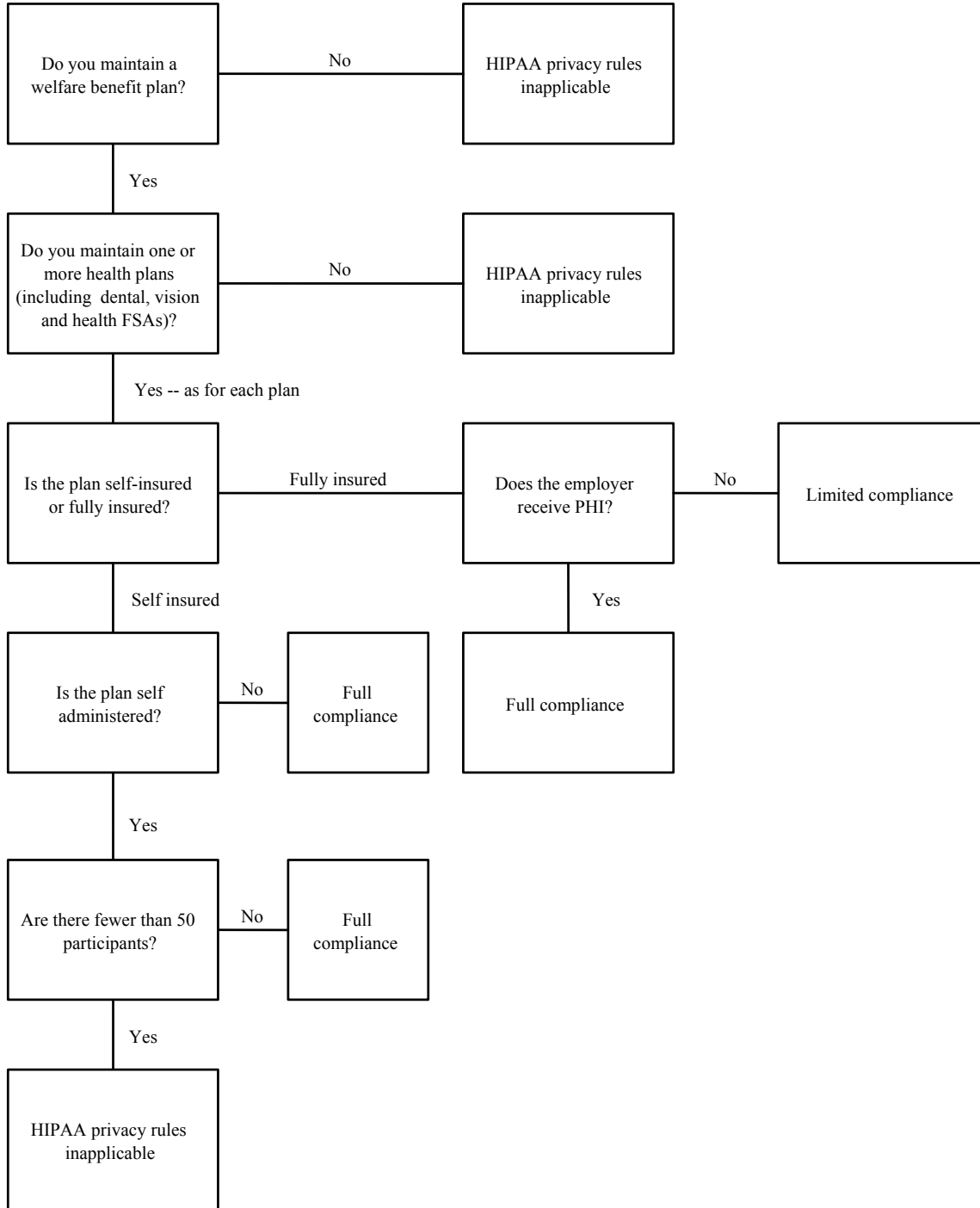
Step 5: Review chart at Appendix C to identify compliance requirements

You might find the following time line helpful, particularly as you review information on the internet, some of which was prepared prior to finalize regulations.



APPENDIX B

HIPAA Privacy Compliance



APPENDIX C

HIPAA Privacy Obligations

Self Funded		Fully Insured	
Fewer than 50 participants and self administered	50 or more participants	No PHI	PHI
No HIPAA privacy obligations	<p>Full HIPAA privacy compliance</p> <ul style="list-style-type: none"> • amend plan to restrict use and disclosure of PHI • designate personnel who will have access to PHI • designate a privacy official • document, implement and train employees on privacy policies and procedures • create firewall to limit access to those designated • provide privacy notice • additional administrative requirements (see advisory) • prohibition on retaliation and waiver • establish procedures to provide for rights of individuals (right of access, right to amend PHI, and right to accounting) • review business associates contracts 	<p>Limited HIPAA privacy obligations</p> <ul style="list-style-type: none"> • insurer has responsibility for HIPAA privacy compliance • prohibition on retaliation and waiver 	<p>Full HIPAA privacy compliance</p> <ul style="list-style-type: none"> • amend plan to restrict use and disclosure of PHI • designate personnel who will have access to PHI • designate a privacy official • document, implement and train employees on privacy policies and procedures • create firewall to limit access to those designated • provide privacy notice upon request • additional administrative requirements (see advisory) • prohibition on retaliation and waiver • establish procedures to provide for rights of individuals (right of access, right to amend PHI, and right to accounting) • review business associates contracts