The Health Insurance Portability and Accountability Act *

**Gary M. Ford and Christy Tinnes**

**Author's Note:**

**I. Introduction**

A. HIPAA, which was signed into law on August 21, 1996, is intended to improve the portability and continuity of health insurance coverage in the group and individual markets.

B. HIPAA guarantees the availability and renewability of health coverage for certain individuals, and it restricts the application of preexisting condition exclusions.

C. HIPAA amends Title I of ERISA, as amended, by adding a new part 7, PHSA, Title XXVII, and IRC §§ 9801 to 9806.

D. The three agencies empowered to interpret and enforce HIPAA—the DOL, the IRS, and HHS—issued interim regulations on the new law on April 1, 1997. 29 C.F.R. part 2590; 26 C.F.R. part 54; and 45 C.F.R. parts 144 and 146, 62 Fed. Reg. 16894 (1997) (to be codified at 29 C.F.R. part 2590, 26 C.F.R. part 54; and 45 C.F.R. parts 144 and 146). The agencies have subsequently issued a number of additional regulations addressing portability, nondiscrimination, and wellness programs.

E. HIPAA also directed HHS to issue standards for confidentiality of individually identifiable health information, security standards for electronic protected health information, and uniform standards and code sets for certain electronic transactions. HHS has enforcement authority over these rules. These rules often are referred to as the HIPAA administrative simplification rules.

F. PPACA, the health care reform law enacted in 2010, expanded many of the provisions under HIPAA and added new insurance market reforms. Generally, these changes were inserted into the existing HIPAA statute and are enforced by the three agencies responsible for HIPAA enforcement—DOL, the IRS, and HHS.

**II. Scope**
A. HIPAA's portability, access, and renewability rules, including the new reforms under PPACA, are applicable to “group health plans” and “health insurance issuers” offering health insurance coverage to “group health plans” and individual coverage. This checklist focuses on the requirements applicable to group health plans.

B. A “group health plan” is defined under HIPAA as an employee welfare benefit plan that provides medical care to employees or their dependents directly or through insurance, reimbursement, or otherwise. ERISA § 733, 29 U.S.C. § 1191b(a); PHSA § 2791(a), 42 U.S.C. § 300gg-91(a); IRC § 9805(a).

1. There are some small differences among the statutes in the definition of a group health plan. For example, the ERISA amendments do not apply to church plans or governmental plans. However, the IRS's definition of group health plan would cover church plans, and the PHSA's definition includes both nonfederal governmental plans and insured church plans.

2. The term “health insurance issuer” is defined as an insurance company, insurance service, or insurance organization (including a health maintenance organization) that is licensed under state law to engage in the business of insurance and is subject to state insurance law. ERISA § 733(b)(2), 29 U.S.C. § 1191b(b)(2); PHSA § 2791(b)(2), 42 U.S.C. § 300gg-91(b)(2); IRC § 9805(b)(2).

3. The term “health insurance coverage” is defined as benefits consisting of medical care under any hospital or medical service policy or certificate, hospital, or medical service plan contract or health maintenance organization contract offered by a health insurance issuer. ERISA § 733(b)(1), 29 U.S.C. § 1191b(b)(1); PHSA § 2791(b)(1), 42 U.S.C. § 300gg-91(b)(1); IRC § 9805(b)(1).

C. The HIPAA administrative simplification rules generally apply to a “covered entity,” which is defined as a health care provider, health care clearinghouse, or health plan. 45 C.F.R. § 160.103. A “health plan” is an arrangement that pays or provides for medical care. This definition generally is broader than the “group health plan” definition found in the HIPAA portability rules.

III. Portability Rules

A. The portability rules are included in the amendments to ERISA, PHSA, and the IRC and limit the extent to which group health plans and health insurance issuers may impose preexisting condition exclusions on participants or beneficiaries.


C. PCE. HIPAA’s PCE rule provides that a group health plan and a health insurance issuer offering group health insurance coverage may not impose a PCE on a participant or beneficiary unless the

(1) PCE relates to a condition for which medical advice or care was recommended or received within a six-month period before the enrollment date;

(2) PCE extends no more than twelve months after enrollment (eighteen months for late enrollees); and

(3) PCE is reduced by the aggregate of the periods of creditable coverage applicable to the participant as of enrollment.
§ 1:33. The Health Insurance Portability and Accountability Act, 1 Checklists for...

a. Coverage under almost any type of plan, policy, or government program qualifies as “creditable coverage.”

b. Periods before a significant break in coverage (sixty-three days) do not have to be credited.

c. A waiting period is not treated as a break in coverage. ERISA § 701, 29 U.S.C. § 1181; PHSA § 2704; IRC § 9801.

d. Under HIPAA, pregnancy is not considered a preexisting medical condition. Furthermore, a PCE may not be imposed on benefits for newborn or adopted children who are covered within thirty days of birth or adoption. ERISA § 701(d), 29 U.S.C. § 1181(d); PHSA § 2704(d); IRC § 9801(d).

E. PPACA changed these rules so that a group health plan no longer may impose a PCE on an individual under age 19 for plan years beginning on or after 9/23/10. A group health plan may not impose a PCE on any individual for plan years beginning on or after 1/1/14. PHSA § 2704. Also beginning in 2014, a group health plan may not impose a waiting period that exceeds 90 days. PHSA § 2708.

F. Certificates of Creditable Coverage. An individual demonstrates prior creditable coverage—to reduce or eliminate a plan's preexisting condition exclusion period—by presenting a certificate of creditable coverage. ERISA § 701(e), 29 U.S.C. § 1181(e); PHSA § 2704(e); IRC § 9801(e).

(1) Plans and issuers are jointly required to provide written certificates to individuals when they lose plan coverage. However, a plan or issuer is deemed to have satisfied the requirement to the extent that another party provides the certificate. A plan may contract with an issuer for the issuer to be responsible for providing certificates.

(2) Certificates generally must include the certificate issue date; the plan name; the participant's or dependent's name and other identifying information; the name, address, and telephone number of the plan administrator or issuer; the telephone number where further information may be obtained; either a statement that an individual has at least eighteen months of coverage without a significant break in coverage, or the date any waiting period or affiliation period began and the date creditable coverage began; and the date creditable coverage ended. The agencies have issued a model certificate.

G. Special Enrollment. The HIPAA portability rules also include “special enrollment” rights for individuals to enroll in group health plan coverage if they have lost other coverage (such as loss of a spouse's employer coverage), have acquired a dependent (such as through marriage, birth, adoption, or placement for adoption), or have become eligible for premium assistance under the Children's Health Insurance Reauthorization Act. A group health plan must allow these individuals to enroll or change elections even outside of annual enrollment.

IV. Nondiscrimination Rules & Wellness Programs


B. HIPAA prohibits a plan from discriminating based on “health-related status” factors. Such factors include an individual's medical condition, claims experience, receipt of health care, genetic information, or disability.
C. The prohibition against discrimination provides that a group health plan and a health insurance issuer may not establish eligibility rules, or charge higher premiums to an individual, based on the individual’s health status.

D. HIPAA does not require a plan to provide particular benefits or prevent a plan from establishing limitations or restrictions on the amount, level, or nature of the benefits or coverage. ERISA § 702(a)(2), 29 U.S.C. § 1182(a)(2); PHSA § 2705(a)(2); IRC § 9802(a)(2). However, this limit or restriction cannot target an individual based on health status.

E. Similarly, HIPAA generally does not limit the premium a plan may charge for coverage to the group as a whole, although a plan may not charge higher premiums to individuals based on health status-related factors. ERISA § 702(b)(1), 29 U.S.C. § 1182(b)(1); PHSA § 2705(b)(1); IRC § 9802(b)(1).

F. A group health plan is permitted to discriminate based on health-related status if the discrimination is in favor of those with an adverse health status (sometimes called benign discrimination).

G. A group health plan also is permitted to discriminate based on health-related status under a wellness program that meets the following rules:

1. The reward for any health-based standard under a wellness program may not exceed 20% of the cost of employee coverage (the employer plus employee contribution). PPACA increases this amount to 30% in 2014. PHSA § 2705.

2. The program must be reasonably designed to promote health or prevent disease.

3. Individuals must be eligible to qualify for a reward at least once per year.

4. The plan must provide a reasonable alternative method to earn the reward for individuals for whom it is unreasonably difficult due to a medical condition, or medically inadvisable, to achieve the health-based standard. The reasonable alternative method must be participation-based and not be health-based. For example, a reasonable alternative method to a requirement to have a certain cholesterol level could be that an individual must exercise once a week.

5. The plan must disclose the availability of the reasonable alternative standard. The final regulations provide sample language.

V. Guaranteed Access and Renewability

A. These guaranteed access rules provide that insurance issuers that offer health insurance coverage in the small group market in a state generally are required to accept every small employer in the state that applies for such coverage, and must accept for enrollment under such coverage every eligible individual who applies for enrollment within the initial enrollment period. PHSA § 2711(a). Under PPACA, this requirements extends to the large group as well in 2014. PHSA § 2702. A small employer generally is defined as an employer who employed an average of at least two, but no more than fifty, employees during the prior calendar year and who employs at least two employees on the first day of the plan year (under PPACA, a state can increase this number to 100 employees). PHSA § 2791(e)(4), 42 U.S.C. § 300gg-12(a).

B. With certain limited exceptions, a health insurance issuer that offers health insurance coverage in either a small or large group market in connection with a group health plan is required by HIPAA to renew or continue in force such coverage at the option of the plan's sponsor. PHSA § 2712(a).
C. Under PPACA in 2014, the insurer also will be subject to rating limitations in the small group market, where the insurer may not adjust premiums except for individual versus family coverage, rating area, age (limit of 3 to 1 ratio), and tobacco use (limit of 1.5 to 1 ratio). PHSA § 2701.

VI. HIPAA Administrative Simplification Rules

A. The HIPAA statute required the Secretary of HHS to issue standards for confidentiality of certain health information and to create uniform standards for sharing this information electronically. These regulations were updated as part of the HITECH Act.

B. HIPAA Privacy Rules. HHS issued the HIPAA Standards for Privacy of Individually Identifiable Health Information in several parts, effective April 14, 2003. 45 C.F.R. Parts 160 to 164. The HIPAA privacy regulations apply to a covered entity, defined as a health plan, health care clearinghouse, or health care provider. The HIPAA privacy regulations cover protected health information (PHI), which is defined as individually identifiable health information.

(1) The HIPAA privacy regulations require covered entities to establish safeguards for PHI, conduct training for workforce members who encounter PHI, and establish procedures to ensure that individuals have a right to access or amend their PHI or obtain an accounting of certain PHI disclosures.

(2) The HIPAA privacy regulations require that a covered entity enter into a business associate agreement with any third party acting on behalf of the covered entity in a function involving PHI. The business associate agreement must require the business associate also to comply with the HIPAA privacy regulations.

(3) The HIPAA privacy regulations require that the covered entity only may use or disclose PHI for the purposes of treatment, payment, or health care operations of the covered entity or pursuant to an exception listed in the regulations. For other disclosures, the covered entity must obtain the individual's written authorization.

(4) There are specific rules governing when a covered entity may disclose PHI to a plan sponsor. Generally, the covered entity only may disclose PHI to a plan sponsor for plan administration functions and only if the plan document has been amended to allow the disclosure and the plan sponsor certifies that it will safeguard the information.

(5) If there is a breach of PHI, and depending on the potential harm involved, the covered entity may be required to notify individuals whose information was breached, the media, and HHS.

C. HIPAA Security Standards. HHS also issued regulations that govern the use and disclosure of electronic PHI. Under the HIPAA Security Standards, the covered entity must establish physical, technical, and administrative safeguards to protect electronic PHI.

D. HIPAA Standard Transactions. Where a covered entity conducts certain transactions with another covered entity using electronic media, the transaction must be conducted using certain standards and code sets established by the Secretary of HHS. The applicable transactions include eligibility, claims, referrals, enrollment, payment, premiums, and coordination of benefits. PPACA made some changes to these rules and required the Secretary to adopt a new transaction for electronic funds transfer.

VIII. Enforcement
A. By amending three independent federal statutes, HIPAA spreads enforcement powers among three federal agencies: the DOL, the HHS, and the IRS.

B. Enforcement through Title I of ERISA. HIPAA does not change ERISA’s current participant remedy provisions. Thus, ERISA § 502(a)(1)(B), 29 U.S.C. § 1132(a)(1)(B), still authorizes any plan participant or beneficiary to sue for recovery of benefits due under the terms of a plan, and prevailing plaintiffs in such suits generally may recover their lost benefits plus attorneys’ fees and costs (but not punitive damages or other “extracontractual” relief).

1. As has always been the case, plan participants and beneficiaries may sue for “appropriate equitable relief” under ERISA § 502(a)(3), 29 U.S.C. § 1132(a)(3), to remedy a violation of Title I of ERISA or the terms of a plan.

2. Because HIPAA puts new substantive rules in part 7 of Title I of ERISA, participants and beneficiaries have standing under ERISA § 502 to enforce HIPAA’s portability provisions.

C. By Plan Fiduciaries or the Secretary of Labor. ERISA § 502(a)(3) and (a)(5), 29 U.S.C. § 1132(a)(3), (a)(5), authorize plan fiduciaries and the Secretary of Labor to sue for appropriate equitable relief to remedy violations of Title I of ERISA and the terms of a plan. New ERISA § 707(b)(3), 29 U.S.C. § 1132(b)(3), clarifies that the DOL’s enforcement authority under ERISA does not extend to health insurance issuers acting only as such. However, the DOL will be able to enforce against third-party administrators and insurers acting as such.

D. Enforcement through the IRC. IRC § 4980D imposes an excise tax penalty on any failure to meet HIPAA’s portability requirements.

1. The tax “shall be” $100 for each day for each individual for whom the failure relates. This is a flat amount, not an “up to” excise tax.

2. The tax is assessed against the sponsoring employer in the case of a single-employer plan and against the plan in the case of a multiemployer plan. There are exceptions for certain small employers or whether the plan can demonstrate that it did not know (and, in exercising reasonable diligence, would not have known) of the failure. There also is an exception where the plan can demonstrate that the failure was due to reasonable cause, rather than willful neglect, and was corrected within 30 days.


E. Enforcement through the PHSA. PHSA §§ 2722(a) and 2761(a), 42 U.S.C. §§ 300gg-22(a) and 300gg-61(a), provide that each state may require health insurance issuers subject to the state’s jurisdiction to meet the new portability, access, and renewability requirements embodied in the PHSA.

1. PHSA §§ 2723(a) and 2762(a), 42 U.S.C. §§ 300gg-23(a) and 300gg-62(a), generally allow for the continued applicability of state laws and remedies, except to the extent they would prevent the application of PHSA’s new substantive requirements.

2. PHSA §§ 2722 and 2761, 42 U.S.C. §§ 300gg-22 and 300gg-61, authorize the Secretary of HHS to enforce PHSA’s provisions.
§ 1:33. The Health Insurance Portability and Accountability Act, 1 Checklists for...

(a) “[i]n the case of a determination by the Secretary that a State has failed to substantially enforce a provision or provisions” of PHSA; and

(b) with respect to group health plans that are nonfederal governmental plans.

3. The Secretary of HHS may assess a civil penalty of up to $100 for each day for each individual for which there is noncompliance. The penalty may be assessed against the health insurance issuer or, in the case of a nonfederal governmental plan, the plan or its sponsoring employer.

F. HIPAA Privacy & Security Rules. Violations under the HIPAA privacy and security rules are subject to a different penalty structure.

1. The Secretary of HHS may impose a penalty of $100 to $50,000 per violation where an entity did not know and would not have known (by exercising reasonable diligence) of the violation. Where the violation is due to willful neglect and not corrected within a 30-day period, the penalty amounts can increase to $50,000 per violation, up to a maximum of $1.5 million.

2. The Secretary also may bring criminal penalties (along with the Department of Justice) of up to $50,000 and/or 1 year imprisonment. If the violation is under false pretenses, the penalty may be up to $100,000 and/or 5 years imprisonment. If for commercial gain, personal gain, or malicious harm, the penalty may be up to $250,000 and/or 10 years imprisonment.

3. State attorneys general may bring civil actions on behalf of residents to enjoin violations and obtain damages of up to $100 per violation, up to $25,000 for identical violations during a calendar year.

4. The Secretary of HHS is required under the HITECH Act to periodically audit covered entities and business associates.


Footnotes

** Gary M. Ford and Christy Tinnes are principals at Groom Law Group, Chartered in Washington, DC (www.groom.com).

* Copyright retained by the authors. All rights reserved. Reprinted with permission.

** Gary M. Ford and Christy Tinnes are principals at Groom Law Group, Chartered in Washington, DC (www.groom.com).