HIPPA and Tax-advantaged Accounts

By Employee Benefits Corporation's
Compliance Department
compliance@ebcflex.com

Date
January 26, 2015

Employee Benefits Corporation

1350 Deming Way, Suite 300
Middleton, WI 53562-4640
P: 800 346 2126 | 608 831 8445
F: 608 831 4790
An employee-owned company
www.ebcflex.com

Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided specific rules and regulations that apply to health plans. HIPAA was designed to improve portability of health plans and to impose privacy and security requirements as it relates to health-related records involved in plan administration. Group health plans were required to comply with HIPAA's portability provisions starting with the plan year that began on or after July 1, 1997[1]. Further, the privacy and security rules and regulations have been amended over the last few years to incorporate technological advances and the growing complexity of health care administration. The accountability in HIPAA is to ensure that a system is in place to identify parties that are responsible to ensure that health information used to deliver, process, or administer the health plan is protected and that those parties are held to a standard. Failure to uphold the standards will result in penalties which may include financial consequences.

This whitepaper provides an explanation of how HIPAA applies to certain tax advantaged accounts, namely health care flexible spending arrangement (health FSAs) and health reimbursement arrangements (HRAs), the significance of the rules on benefit plan administration and the consequences of non-compliance.

HIPAA Provision Applicability and Exceptions

While HIPAA has broad application to health plans, it is important to understand that some plans that an employer offers to its employees are exempt from HIPAA (HIPAA does not apply), that others may be excepted benefits (subject to HIPAA but not required to comply with some of HIPAA's requirements) and that some plans are non-excepted benefits (all of the HIPAA requirements apply).

Exempt From HIPAA. Plans that provide only certain incidental types of nonmedical benefits are exempt from HIPAA entirely (e.g. accident, disability income, liability and worker's compensation coverage).

Excepted from the HIPAA Portability Requirements. Health FSAs that qualify as an excepted benefit[2] are not be subject to HIPAA's portability requirements (including pre-existing condition exclusions (PCEs), special enrollment rights and nondiscrimination rules). Further, there is an exception for stand-alone limited-scope dental or vision benefits as long as the dental or vision coverage is provided separately from the medical plan coverage. Generally, this means that employees elect to participate in such coverage separately from the medical plan coverage. HRAs that provide dental or vision benefits, only, are also excepted from the HIPAA portability requirements. Finally, plans that cover only former employees, such as separated or retired employees are excepted from the portability requirements.

HIPAA's Privacy and Security Requirements. Self-administered, self-insured group health plans, including health FSAs and HRAs, with fewer than 50 employees eligible to participate are not subject to HIPAA's administrative simplification rules, including the privacy and security requirements. This exemption is not applicable for plans that use a third party administrator for claims processing or for

[1] HIPAA §§101(g), 102(c), and 401(c)

[2] Code §§ 9831 (b) and (c), PHSA §2722

limited-scope dental or vision benefits. The privacy and security requirements apply in these cases, even though they are excepted from HIPAA's portability requirements.

HIPAA's Impact on Group Health Plans

All group health plans are impacted by the HIPAA regulations. A group health plan is a plan that provides health care and is maintained by an employer.[3] For example, group health plans include health insurance, dental insurance, and vision insurance. Some tax advantaged accounts are also subject to HIPAA. While a cafeteria plan is not subject to the HIPAA provisions, the underlying health FSA is a self-funded health plan that is subject to some of the rules. An HRA is also a self-funded health plan subject to HIPAA.

Enforcement of HIPAA Rules and Potential Penalties

The HIPAA portability rules are enforced jointly by the IRS, the Department of Labor (DOL) and the Department of Health and Human Services (HHS). The privacy and security rules are enforced by HHS, through its Office for Civil Rights. IRS Code §4980D imposes an excise tax for a group health plan's failure to comply with HIPAA's portability requirements contained in the Code.[4] If a plan is found to not comply with the HIPAA regulations, the employer sponsoring the plan may be subject to financial penalties and lawsuits.

The potential penalties include:

- An IRS excise tax of $100 per day of noncompliance per individual affected imposed on the plan sponsor [5]
- Civil action
- Civil penalties of $100 to $50,000 per violation with a maximum of $1.5 million per year per provision violated
- Criminal penalties for knowing violation
- Private party lawsuits

Excise taxes can be substantial. The minimum excise tax for a compliance failure discovered after a notice of examination generally is $2,500.[6] The minimum excise tax is increased to $15,000 if violations are "more than de minimis."[7] The maximum excise tax for "unintentional failures" for a single employer plan is the lesser of 10% of the amount paid during the preceding tax year by the employer for group health plans, or $500,000.[8]

[3] *See* **Code §9832(a)** (by reference to **Code §5000(b)(1)**; **ERISA §733(a)(1)**; **PHSA §2791(a)(1)**).
[4] Code §4980D(e)(1)
[5] Code §4980D(e)(1)
[6] Code §4980D(b)(3)(A).
[7] Code §4980D(b)(3)(B). Neither the $2,500 minimum nor the $15,000 minimum applies to a church plan. Code §4980D(b)(3)(c).
[8] Code §4980D(c)(3)(A).

HIPAA and Third Party Administrators (TPA)

If the employer contracts with a third party to help with the administration of their plan, the third party assumes some of the same liabilities as the covered entity with respect to HIPAA. These third parties (TPA) are known as business associates.[9] Employee Benefits Corporation would be a business associate of the BESTflex and EBC HRA plans when the employer/plan sponsor has contracted with Employee Benefits Corporation to provide plan administration services that includes health care FSA and/or HRA claims review and payment.

Although the employer may contract with a TPA for plan operations for a health FSA and/or HRA or provide health plan coverage that is fully insured, there may be times when an employer gets involved with helping an employee resolve a claims issue. An employer can help the employee resolve claims disputes if the PHI is provided by the employee or if the PHI comes from the provider and there is a written authorization on file from the insured that names the employer as an authorized representative.

In order for the covered entity to not violate the HIPAA Privacy and HIPAA Security rules, the covered entity must obtain satisfactory assurances from the business associate in order for them to share any PHI for purposes of operation of the plan. Typically, this assurance is in the form of a written agreement, commonly known as the HIPAA Business Associate Agreement (BAA).

The HIPAA BAA must provide the specific details of the HIPAA provisions and outline the responsibilities that are applicable to the business associate and the covered entity. In addition, if the business associate has business associates, then agreements must be in place in order for the business associate to sub-contract certain aspects of administration to yet another third party.[10] It is also necessary to include a provision in the HIPAA BAA with the covered entity to detail out what HIPAA provisions the business associate's sub-contractor is expected to abide by so that the covered entity is not at risk of violation due to the business associate's sub-contractor's actions.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.[11] The final HITECH rules were published on January 23, 2013 with general compliance to be effective September 23, 2013. The HITECH Act significantly changed how the privacy and security standards apply to business associates. Business associates are held to the same standard as the health plans for purposes of the security provisions and contractually obligated for purposes of privacy. Although covered entities and business associates have somewhat different notice obligations, each must be able to identify breaches in order to satisfy its respective obligations.[12]

[9] 45 CFR §160.103.
[10] 45 CFR §160.103 (paragraph (3) of business associate definition).
[11] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009).
[12] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009), §13402

HIPAA Portability Provisions

HIPAA's portability requirements will generally apply to group health plans and the insurers that issue group health plan coverage. Some health FSAs and limited-scope dental and vision plans are excepted from the portability provisions. The Affordable Care Act (ACA)[13] makes significant changes to HIPAA's portability requirements, which includes changes to preexisting condition exclusions (PCE), nondiscrimination rules, additional provisions relative to lifetime and annual dollar limits and the prohibition on rescissions. The effective dates of these changes are varied.

1. **Preexisting Condition Exclusions (PCE)**[14] HIPAA restricts the length of time that a group health plan may review to determine if an individual has a preexisting condition and also states that an individual must have received this diagnosis or care by a licensed professional in order to be considered.

   Also, to ensure continuous coverage for an individual with a preexisting condition, this provision outlined the need for a health plan to issue a Certificate of Creditable Coverage upon termination of the plan or coverage.

   This portion of the portability provision is almost obsolete due to provisions in the Affordable Care Act (ACA). [15] There is a prohibition on preexisting condition clauses for health plans issued or renewing on or after January 1, 2014. For this reason, Certificates of Creditable Coverage will no longer be necessary after January 1, 2015.[16]

2. **Special Enrollment Rights** [17] In certain circumstances, HIPAA gives individuals a window of opportunity to enroll if they had previously waived coverage. The length of time varies dependent upon the circumstance and for those enrolling in the plan under special enrollment provisions they are not treated as late enrollees.

   These special enrollment rights must be spelled out in the summary plan description and provided to individuals when they are first eligible to enroll. Examples of special enrollment opportunities are as follows:

   a. **Loss of Other Coverage.**[18] If an individual exhausts their COBRA benefit because they have reached the maximum coverage period, loses eligibility for coverage under another plan or the employer contributions for their plan cease, the plan is required to allow an individual the right to enroll as long as that enrollment is requested within 30 days of the loss.

[13] Patient Protection and Affordable Care Act, **Pub. L. No. 111-148** (2010) (PPACA), as amended by the Health Care and Education Reconciliation Act of 2010, **Pub. L. No. 111-152** (2010) (HCERA)
[14] Treas. Reg. §54.9801-3(a)(1)(i); DOL Reg. §2590.701-3(a)(1)(i); HHS Reg. §146.111(a)(1)(i).
[15] PHSA §2704(a), as amended by PPACA, Pub. L. No. 111-148, §1201 (preexisting condition exclusion) and §1255 (effective date) (2010).
[16] PHSA §2704(a), as amended by PPACA, Pub. L. No. 111-148, §1201 (preexisting condition exclusion) and §1255 (effective date) (2010).
[17] Code §9801(f); ERISA §701(f); PHSA §2704(f).
[18] Treas. Reg. §54.9801-6(a)(2); DOL Reg. §2590.701-6(a)(2); HHS Reg. §146.117(a)(2).

If a plan covers same-sex spouses and/or domestic partners of employees, then an employee's same-sex spouse or domestic partner will qualify as a dependent for HIPAA special enrollment if the same-sex spouse or domestic partner loses other health coverage. This rule is unaffected by the U.S. vs. Windsor decision[19], as the domestic partner's or same-sex spouse's statutory right to special enrollment is based on his or her status as an eligible dependent under the plan. It is not determined by his or her status as a spouse under federal law.

The timeframe is increased to 60 days if that loss is under a Medicaid plan or a state's children's health insurance program.

The coverage for the new plan begins on the first of the month following the enrollment request.

b. **Eligible for State Premium Assistance.**[20] If an individual becomes eligible for a subsidy under a state's Medicaid plan or a state's children's health insurance program (CHIP), the individual has 60 days to request to enroll.

c. **Acquisition of New Dependent.**[21] If an individual acquires a new spouse or dependent through marriage, birth, adoption or placement for adoption, the plan has to allow the employee, the employee's spouse and the newly acquired dependent to enroll in the plan as long as that enrollment is requested within 30 days of the event.

   The plan does not have to allow the existing dependents to enroll if they were not already enrolled.

   The coverage for the new plan begins on the first of the month following the enrollment request if the event was a marriage. The coverage for the new plan is retroactive to the event date in the event of birth, adoption or placement for adoption.

HIPAA's special enrollment rights also apply to COBRA qualified beneficiaries (QB) who are enrolled in COBRA coverage under the plan. Therefore, COBRA QB's have the same right to enroll family members as if the QB were an active employee participating in the plan.[22]

3. **Nondiscrimination Rules**[23] HIPAA states that group health plans and health insurers are not allowed to discriminate based on a health status-related factor for purposes of eligibility, premiums or contributions.

[19] *U.S. v. Windsor*, 2013 WL 3196928 (U.S. 2013).
[20] Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. No. 111-3, §311 (2009).
[21] Code §9801(f)(2); ERISA §701(f)(2); PHSA §2704(f)(2); Treas. Reg. §54.9801-6(b); DOL Reg. §2590.701-6(b);HHS Reg. §146.117(b).
[22] Treas. Reg. §54.4980B-5, Q/A-5(a).
[23] Treas. Reg. §54.9802-1(b)(1)(i); DOL Reg. §2590.702(b)(1)(i); HHS Reg. §146.121(b)(1)(i).

Health status-related factors include medical conditions, claims experience, medical history, genetic information (GINA), evidence of insurability and disability.

Wellness incentives must satisfy certain criteria to avoid being discriminatory. Beginning in 2014 due to health care reform, wellness incentives are allowable as long as the reward is no more than 30% for general health-contingent programs and up to 50% for standards related to tobacco use, it is designed to promote health or prevent disease, it gives individuals the opportunity at least once a year, reward is available to all similarly situated individuals and reasonable alternative and waivers are available.[24]

Also, discriminating *in favor of* individuals with adverse health conditions is allowable.

a. **Eligibility Discrimination.** Excluding individuals from participating because they are out on medical leave, participate in dangerous activities or have a history of medical problems and high health claims are all prohibited.

b. **Premium Discrimination.** Charging an individual more for their premiums because they have a chronic medical condition or discounting an individual for having small medical claims are prohibited.

c. **Contribution Discrimination**. The employer paying less of a premium for an individual because they have a chronic medical condition or discounting an individual for having small medical claims is prohibited.

HIPAA Privacy and Security Provisions

Under HIPAA, the privacy and security provisions are known as the Administrative Simplification requirements.[25] Under HIPAA's administrative simplification provisions, a health plan is an individual plan or a group plan that provides (or pays the cost of) medical care.[26] HIPAA's definition of group health plan is tied to the ERISA definition of an employee welfare benefit plan.[27] In the event that a wrap plan exists, the plan document will generally define the number of plans for HIPAA purposes. Although certain excepted benefits like some health care FSA and limited-scope dental and vision plans can avoid the HIPAA portability rules, the plan remain subject to the privacy and security provisions.

Group health plans, clearinghouses, providers and any third parties that access protected health information must comply and are known as covered entities. Employers typically will not be covered entities; however, the health plans they sponsor will be subject to the rules and thereby they will be responsible for the HIPAA compliance. The HIPAA privacy rule applies to protected health information (PHI) and the security rules apply to electronic PHI (e-PHI). If an employer performs any administrative

[24] Incentives for Nondiscriminatory Wellness Programs in Group Health Plans, 26 CFR Part 54, 29 CFR Part 2590, 45 CFR Parts 146 and 147, 78 Fed. Reg. 33158, 33161 (June 3, 2013).
[25] 42 U.S.C. §1320d
[26] SSA §1171(5); 45 CFR §160.103
[27] SSA § 1171(5)(A).

functions for the group health plan that involves health plan claims review and payment the employer will be further responsible for HIPAA privacy and security requirements.

Protected health information (PHI) is any "individually identifiable health information." This includes any identity markers (such as name, social security number, patient number, date of birth, etc.) that exist on a document, electronic or otherwise, along with health information (such as claims payment amounts, medical information, dates of service, etc.)

1. **Privacy Standards.**[28] The privacy standards define use and disclosure rules. Covered entities generally cannot disclose PHI for any reason not identified in HIPAA unless there is specific written consent. Examples of acceptable disclosures that do not require an authorization include disclosure for purposes of treatment, operations and payment of claims. There are also other circumstances where it might be disclosed for judicial proceedings or for public safety reasons.
   These use and disclosure standards also indicate that individuals only have access to information that is "minimally necessary" for them to complete their duties. This includes computerized restrictions as well as physical patient files.

   Under the privacy standards, there is the requirement to provide individuals with a notice of their rights and of privacy practices. Providers and health plans must provide this notice. For self-funded plans like *health FSA and HRA it would be the employer's responsibility* and for insured plans the notice is the responsibility of the insurance carrier.

   There must also be written privacy standards for covered entities that include training procedures and violation protocols.

2. **Security Standards**.[29] Covered entities must have appropriate electronic security to protect PHI. These standards are categorized into administrative safeguards, physical safeguards, technical safeguards, organizational requirements and policies, procedures and documented requirements.

   In general, the security rule requires covered entities (including group health plans) to:

   - ensure the confidentiality, integrity, and availability of all electronic PHI that the covered entity creates, receives, maintains, or transmits;
   - protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI;
   - protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted or required under the privacy rule; and
   - ensure compliance with the security rule by the covered entity's workforce.[30]

   The regulations sometimes address specifically what needs to be implemented, but other times, the degree of implementation is left to the covered entity. The covered entity must assess their risk,

[28] HIPAA §264(b).
[29] SSA §1173(d)(2)
[30] 45 CFR §164.306(a).

their technology and current security practices and determine whether or not they need to update or upgrade.

HIPAA Breach Notification Process and Procedure

A breach is defined as the "acquisition, access, use or disclosure" of PHI in a manner not permitted under the privacy rule that "compromises the security or privacy" of the PHI, subject to specified exceptions.[31]

"Use" is defined as "the sharing, employment, application, utilization, examination, or analysis of [PHI] within an entity that maintains such information," and "disclosure" is "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information."[32]

An "acquisition" could be either a use or a disclosure, depending on who acquired the PHI—e.g., a workforce member (inside) or a business associate (outside). [33]

Based upon the 2013 final regulations, a covered entity or business associate must presume that an acquisition, access, use, or disclosure of PHI in violation of the privacy rule is a breach. This will hold true unless the business associate can demonstrates that there is a "low probability" that the PHI has been compromised based on a risk assessment.

The risk assessment must consider at minimum the following factors:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.[34]

Breaches are reportable only if the impermissible use or disclosure involves "unsecured protected health information." [35] Unsecured PHI means PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or method specified by Health and Human Services (HHS)." [36] Encryption and destruction are the only two methods identified for rendering PHI unusable, unreadable or indecipherable.[37]

[31] 45 CFR §164.402
[32] 45 CFR §160.103
[33] Final Rule, 78 Fed. Reg. 5565, 5645 (Jan. 25, 2013).
[34] 45 CFR §164.402
[35] 45 CFR §164.408(a).
[36] 45 CFR §164.402
[37] Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

Covered entities and business associates need to evaluate the facts and circumstances to determine if a breach has occurred by considering the following:

1. Determine if under the privacy rule there has been an impermissible use or disclosure of unsecured PHI.
2. Determine if the any of the breach exceptions are applicable. Breach exceptions include unintentional acquisition, use or access of PHI by a workforce member, inadvertent disclosure from one authorized person to another, unauthorized disclosure where reasonable to believe information will not be retained.
3. If no exception is applicable, determine and document whether the impermissible use or disclosure causes the PHI to be compromised. The risk assessment factors described earlier in this section will help evaluate the situation.

A breach is considered discovered when the incident becomes known, not when the covered entity or business associate concludes the analysis of whether the facts constitute a breach.[38] You are required to notify parties that a breach has occurred without an unreasonable delay, however, you have no more than 60 days from when the breach is discovered to make this notification. [39] In the event that more than 500 residents of a state are involved with a single breach, in addition the media must be notified of the breach.[40] Covered entities are typically responsible for breach notification; however they contractually could make this a business associate responsibility. Health and Human Services (HHS) must be notified of breaches of less than 500 incidents annually and at the time of occurrence if more than 500 people are involved in any single breach.[41]

Looking Ahead

There are some changes on the horizon for 2014 and 2015. On April 27, 2012, in accordance with an Affordable Care Act (ACA) requirement [42] HHS proposed regulations establishing a standard for a national unique health plan identifier (HPID) and provisions for implementation of the HPID. On September 5, 2012, HHS published final HPID regulations that included little change to the detail from the proposed regulations; however, there were changes to the implementation dates.[43]

The Centers for Medicare and Medicaid Services (CMS) on September 30, 2014, published a Q & A Document clarifying which health plans need a health plan identifier (HPID), who must apply for the HPID and the deadline date for having a HPID for an affected health plan. [44]

[38] 74 Fed. Reg. 42740, 42748 (Aug. 24, 2009)
[39] 45 CFR §164.404(b)
[40] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009), §13402(e)(2); 45 CFR §164.406(a).
[41] HHS-OCR Breach Notification Rule: Instructions for Submitting Notice of a Breach to the Secretary
[42] PPACA, Pub. L. No. 111-148, §1104(c)(1) (2010)
[43] Final Rule, 77 Fed. Reg. 54664 (Sept. 5, 2012)
[44] https://questions.cms.gov/faq.php?isDept=0&search=HPID&searchType=keyword&submitSearch=1&id=5005

Q&A number ten clarifies that a HPID is not needed for a health FSA or for a health reimbursement arrangement (HRA) that reimburses deductible or other out-of-pocket expenses associated with the employer's group medical plan (e.g., an integrated HRA).[45]

Consequently, the only HRAs that require an HPID are stand-alone HRAs that reimburse more than dental or vision expenses, HRAs that conduct covered transactions electronically with a covered entity, and an HRA that reimburses retirees for their medical expenses and/or premiums is an example of a stand-alone HRA that needs a HPID.

Since the employer self-insures the affected HRA, the employer will need to apply for the HPID and use the 10-digit identifier when performing standard transactions by the required date based on the size (amount of reimbursement) of the HRA. Large HRAs – those that reimburse over $5 million per year - need the HPID by November 5, 2014. Small HRA plans need their HPID by November 5, 2015.

Note: Effective October 31, 2014, the Centers for Medicare & Medicaid Services (CMS) Office of e-Health Standards and Services (OESS), the division of the Department of Health & Human Services (HHS) that is responsible for enforcement of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) standard transactions, code sets, unique identifiers and operating rules, announces a delay, until further notice, in enforcement of 45 CFR 162, Subpart E, the regulations pertaining to health plan enumeration and use of the Health Plan Identifier (HPID) in HIPAA transactions adopted in the HPID final rule (CMS-0040-F). [46]

On September 23, 2014, the National Committee on Vital and Health Statistics (NCVHS), an advisory body to HHS, recommended that HHS rectify in rulemaking that all covered entities (health plans, healthcare providers and clearinghouses, and their business associates) not use the HPID in the HIPAA transactions (see http://ncvhs.us/wp-content/uploads/2014/10/140923lt5.pdf). This enforcement discretion will allow HHS to review the NCVHS's recommendation and consider any appropriate next steps.[47]

This enforcement delay applies to all HIPAA covered entities, including healthcare providers, health plans, and healthcare clearinghouses.

Conclusion

Employee Benefits Corporation is a business associate when an employer/plan sponsor enters into a service agreement for BESTflex and EBC HRA administration that includes health claims review and payment. We use protected health information (PHI) for plan operations. Operations such as claims substantiation is a requirement for reimbursement under IRS tax code in addition to application under

[45] https://questions.cms.gov/faq.php?isDept=0&search=HPID&searchType=keyword&submitSearch=1&id=5005
[46] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/Affordable-Care-Act/Health-Plan-Identifier.html

[47] http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/Affordable-Care-Act/Health-Plan-Identifier.html

HIPAA. The privacy rights and the security of plan information and participant PHI is very important to us. We have taken the required steps to comply with HIPAA and HITECH and regularly evaluate our systems and practices to ensure continued compliance.

Employee Benefits Corporation

1350 Deming Way, Suite 300
Middleton, WI 53562-4640
P: 800 346 2126 | 608 831 8445
F: 608 831 4790
An employee-owned company
www.ebcflex.com

