Compliance Overview

Highlights

HIPAA Rules

- The HIPAA Rules impose standards for the privacy and security of PHI.
- The HIPAA Rules apply directly to health plans, health insurance issuers and business associates.
- The impact of the HIPAA Rules on a specific employer's health plan depends on how the plan is funded and whether the employer has access to PHI.
- The HIPAA Rules do not apply to an employer's employment-related records.

Compliance Steps

Key compliance steps include:

- Identifying each health plan and its funding;
- Looking for access to PHI;
- Considering the impact of wellness programs;
- Implementing appropriate safeguards; and
- Reviewing Privacy Notice requirements.

Bolton

What Employers Should Know About HIPAA Privacy

The Health Insurance Portability and Accountability Act (HIPAA) is a broad federal law that protects the privacy and security of personally identifiable health information, known as protected health information (PHI). The HIPAA Privacy and Security Rules (HIPAA Rules) apply to covered entities, including health plans and health insurance issuers, and to business associates performing functions on behalf of covered entities involving PHI.

The HIPAA Rules do not directly apply to employers or to employment-related records, even those that contain medical information. However, other federal laws, such as the Americans with Disabilities Act (ADA) and the Family and Medical Leave Act (FMLA), include confidentiality requirements for employees' medical information.

Although employers are not directly regulated by HIPAA, the HIPAA Rules apply to them through their role as health plan sponsors. Compliance obligations vary considerably depending on whether a health plan is self-funded or fully insured and the employer's involvement in plan administration. Employers sponsoring fully insured plans with limited access to PHI have minimal obligations, while those administering self-funded plans have more responsibilities.

This Compliance Overview provides employers with a practical step-by-step guide to understanding their HIPAA compliance obligations.

Links and Resources

The U.S. Department of Health and Human Services (HHS) oversees the HIPAA Rules. Review the following links for more information:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA compliance and enforcement

Compliance Overview

Step One: Identify Health Plans and Funding

Because the HIPAA Rules directly apply to health plans, employers should **identify their health plans** as an initial compliance step. In general, all employer-sponsored plans that provide or pay for healthcare are subject to the HIPAA Rules. The following table provides examples of common employer-sponsored welfare benefits and indicates whether they are considered health plans subject to the HIPAA Rules.

Type of Welfare Benefit	Subject to HIPAA Rules?
Medical plans	Yes
Dental and vision plans	Yes
Prescription drug plans	Yes
Health flexible spending accounts (FSAs)	Yes
Health reimbursement arrangements (HRAs)	Yes
Individual coverage HRAs (ICHRAs)	Yes
Excepted benefit HRAs (EBHRAs)	Yes
Qualified small employer HRAs (QSEHRAs)	Yes
Dependent care FSAs	No
Adoption assistance FSAs	No
Health savings accounts (HSAs)	No, but the high deductible health plans (HDHPs) offered with HSAs are subject to the HIPAA Rules
Disease-specific policies, such as cancer policies	Yes, if they provide coverage for medical care
Life insurance	No
Disability insurance	No
Section 125 premium-only plans	No

Also, a health plan's funding impacts the scope of an employer's HIPAA obligations for the plan. In addition to identifying their health plans, employers should **confirm whether each health plan is fully insured or self-funded**. Employers with self-funded health plans have significant compliance obligations under the HIPAA Rules. In contrast, the compliance responsibility for fully insured health plans may be minimal, particularly when the employer does not receive PHI from the issuer for plan administration purposes.

Also, there is a special exemption for certain small, self-funded health plans. Under this exemption, a self-funded health plan with **fewer than 50 participants administered by the employer** sponsoring the plan is not subject to the HIPAA Rules.

Step Two: Look for Access to PHI

The HIPAA Rules protect PHI that is held or transmitted by a regulated entity, including a health plan, healthcare provider or business associate. PHI includes information that identifies the individual (or for which there is a reasonable basis to believe it can be used to identify the individual) and relates to:

- The individual's past, present or future physical or mental health or condition;
- The provision of healthcare to the individual; or

- The past, present or future payment for the provision of healthcare to the individual.

Some employers, especially those with self-funded health plans, receive PHI from their third-party administrators (TPAs), issuers or other service providers for plan administration purposes (e.g., reviewing claims decisions). **When an employer has access to PHI for health plan administrative functions, it increases the employer's HIPAA compliance obligations.** For example, the employer must implement appropriate administrative, physical and technical safeguards to protect the privacy and security of PHI and train their workforce on privacy and security policies. Also, the employer cannot use PHI from the health plan in any employment-related action or decision or in connection with any other benefit plan.

Significantly, **PHI does not include employment records held by an employer**, such as records related to occupational injury, leave requests, drug screenings, reasonable accommodation requests and fitness-for-duty examinations. Medical information that an employee discloses to their employer is generally not subject to the HIPAA Rules, even if it is prepared by a healthcare provider. However, because most healthcare providers are subject to the HIPAA Rules, a HIPAA authorization is required for a healthcare provider to directly release an employee's medical information to the employer. Once this information is released to the employer, it is no longer subject to the HIPAA Rules, although other laws impose confidentiality requirements on employees' medical information, such as the ADA and the FMLA.

Step Three: Consider Wellness Programs

Whether the HIPAA Rules apply to a wellness program depends on its structure. Some employers offer wellness programs to their employees as part of their group health plan. For example, employers may offer incentives or rewards related to group health plan benefits, such as reduced premiums or cost-sharing amounts, in exchange for participation in a wellness program. Other employers may offer workplace wellness programs directly and not in connection with a group health plan.

- **When a wellness program is offered as part of a group health plan**, any individually identifiable health information collected from or created about participants in the wellness program is PHI and protected by the HIPAA Rules. HIPAA also protects PHI held by the employer on the plan's behalf when the employer administers aspects of the plan, including wellness program incentives offered through the plan.
- **When a workplace wellness program is offered by an employer directly and not as part of a group health plan**, the health information that is collected from employees by the employer is not protected by the HIPAA rules. However, other federal or state laws may apply and regulate the collection and use of the information.

Employers with wellness programs subject to the HIPAA Rules should ensure they have **business associate agreements** in place with their wellness vendors if the programs involve the collection or creation of individually identifiable health information. They should also implement appropriate safeguards for the PHI, as explained below.

Step Four: Implement Appropriate Safeguards for PHI

Depending on the extent of their HIPAA compliance obligations, employers may be required to implement safeguards to protect the privacy and security of PHI. For example, if an employer has a self-funded health plan, or they have a fully insured health plan and receive PHI for plan administration purposes, the employer must amend their health plan documents and certify that they agree to, among other things:

- Establish adequate separation between employees who perform plan administration functions and those who do not;
- Not use or disclose PHI for employment-related actions or other purposes not permitted by the HIPAA Rules;
- Where electronic PHI is involved, implement reasonable and appropriate administrative, technical and physical safeguards to protect the information, including by ensuring that there are firewalls or other security measures in place to support the required separation between plan administration and employment functions; and

- Report any unauthorized use or disclosure, or other security incident, of which they become aware.

Other protections required by the HIPAA Rules include entering into agreements with business associates who create, receive or maintain PHI on behalf of the health plan, designating privacy and security officials, and adopting related policies and procedures.

Employers with fully insured health plans typically do not perform administrative functions involving PHI on behalf of the plan. When an employer's only exposure to PHI consists of enrollment data, summary health information and information disclosed through a HIPAA authorization, the bulk of HIPAA compliance responsibilities shift to the health insurance issuer rather than the employer-sponsored group health plan. As a result, these employers face relatively few obligations under the HIPAA Rules. However, as explained above, sponsoring a wellness program that is offered as part of the health plan may trigger additional HIPAA compliance responsibilities.

Step Five: Review Privacy Notice Requirements

The HIPAA Rules require certain health plans and issuers to provide a Notice of Privacy Practices to plan participants. The Privacy Notice must be written in plain language and must:

- Explain how the health plan or issuer may use and disclose an individual's PHI;
- Describe the individual's rights with respect to their PHI; and
- Summarize the health plan's or issuer's legal duties with respect to the PHI.

HHS has provided a model Privacy Notice for health plans and issuers to use.

The Privacy Notice requirements for an employer's health plan vary depending on whether the plan is self-funded or fully insured, and, if the plan is fully insured, whether the plan sponsor has access to PHI for plan administration purposes, as explained in the following table:

Type of Health Plan	Privacy Notice Requirements
Self-funded health plans	Employers with self-funded health plans must provide a Privacy Notice to new enrollees at the time of enrollment, within 60 days of a material change to the notice, and upon a participant's request. Also, at least once every three years, the Privacy Notice must be redistributed, or participants must be notified that the notice is available with instructions for obtaining a copy.
Fully insured health plans	The issuer has the primary responsibility for a fully insured plan's Privacy Notice. However, employers with fully insured health plans that access PHI for plan administration purposes must maintain a Privacy Notice for the plan and provide it upon request. Employers without access to PHI (other than enrollment information, summary health information and information released pursuant to a HIPAA authorization) are **not required** to maintain or provide a Privacy Notice.