

HIPAA Privacy Regulations and Protections

Question: What is this all about?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. The privacy regulations are part of HIPAA Administrative Simplification. Administrative Simplification is intended to make health care administration (including payment) more efficient by providing for the adoption of uniform data sets and code sets for health care transactions such as claims and by encouraging the use of electronic data interchange.

There are privacy and security concerns because so much sensitive health care information is moved electronically during standard transactions. The privacy regulations aim to keep such information from being used or disclosed improperly.

Question: Is American Eagle, as my employer, covered by the privacy regulations?

No. The regulations do NOT apply to employers except when the employer is acting in its capacity as the sponsor of the health plan.

This means that when American Eagle is acting as the employer and implementing or enforcing work rules like requiring a Doctor's note following an absence or requiring detailed health related information to AA Medical when applying for Family Leave, HIPAA **does not apply**.

Question: What other protections might an employee have?

American Eagle has its own privacy policy it can be found on JetNet in the Benefits section of the website. Additionally, there may be State privacy statutes that might offer protection of personal medical information and employment records.

Question: What is Protected Health Information?

Protected health information (PHI) individually identifiable information created (in any form) or received by certain health and welfare plans sponsored by American Eagle. Examples of PHI are: explanation of benefits, claims information given by the individual over the phone to a Benefits Administration person, types of health service provided, and reports with information on individual claims, including the cost of any health service provided.

Question: Can my PHI be shared in the case of an injury on duty?

If you participate in the Group Life and Health Benefits Plan (the "Plan") at American Eagle, then the Plan may disclose your PHI as authorized by you or your representative and to the extent necessary to comply with laws relating to Workers' Compensation and similar programs providing benefits for work-related injuries or illnesses if either: (1) the health care provider is a member of the employer's workforce and provides health care to the individual at the request of the employer, the PHI is provided to determine if the individual has a work-related illness or injury or to provide medical surveillance of the workplace, and the information is required for the employer to comply with OSHA or with laws with similar purposes, or (2) you authorize the disclosure. You must authorize the disclosure in writing and you will receive a copy of any authorization you sign.

Question: Are there other circumstances when my PHI may be disclosed without my authorization?

Once again, if you are a Plan participant, then American Eagle may be required to disclose or use your PHI for certain other purposes. For example, disclosure may be required if certain types of wounds occur or to comply with a court order, a warrant, a subpoena, a summons, or a grand jury subpoena.

Question: To what entities do the privacy regulations apply?

The regulations apply to three kinds of "covered entities": health care clearinghouses, health plans, and health care providers that conduct any of the standard transactions electronically.

Health Care Clearinghouses: Clearinghouses are entities that "translate" health information from a non-standard format to standard, or vice versa. Examples are billing services and re-pricing companies.

Health Plans: Health plans are individual or group plans that provide or pay for the cost of medical care. Health Plans include HMOs, Medicare, Medicaid, health insurance issuers, and group health plans. The only health plans that are not covered now are group health plans that have fewer than 50 participants and are administered entirely by the plan sponsor.

Health Care Providers: As the term implies, these are persons or organizations that provide medical or health services or that bill or are paid for health care in the normal course of business. Only providers that conduct any of the HIPAA standard transactions (e.g., health care claims or encounter information; eligibility inquiry; request for authorization to refer a patient to another provider, etc.) electronically are required to comply with the HIPAA privacy regulations.

Other Entities with HIPAA Privacy Obligations:

There are two other entities that may have HIPAA privacy obligations even though they are not "covered entities". These are: business associates of covered entities, and plan sponsors.

Obligations are imposed on business associates by contract and through business associate contracts with covered entities. Obligations are imposed on a plan sponsor (in order to obtain protected information from the plan) by (i) required plan amendments, (ii) a certification by the sponsor, and (iii) assurances of adequate separation between plan functions and employer functions.