

## Benefit Fact Sheet

### Objective

In 1999, under Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Department of Health and Human Services (HHS) issued the first comprehensive federal protection for the privacy of health information known as the HIPAA Privacy Rule. In an effort to prevent inappropriate uses and disclosures, the Privacy Rule applies certain restrictions to the use and disclosure of protected health information (PHI).

### Why offer it?

Failure to comply may result in civil monetary penalties including fines and prison terms for misuse of patient information with knowledge and intent.

### Who offers it?

All health plans, insurance issuers, providers and clearing houses are by definition covered entities and must comply. Plans with fewer than 50 employees that are self-insured and self-administered by the employer, as well as plans whose primary benefits are not health benefits are considered an exception.

Some or all of HIPAA's administrative simplification rules also apply indirectly to employers/plan sponsors that perform administration functions for the group health plans they sponsor, if the administration functions involve PHI. As the sponsor of a group health plan, the employer is now considered a Covered Entity and is required to comply with the HIPAA Privacy and Security Rules.

The Department of Labor released further clarification indicating that employers with fully-insured plans who do not create or receive PHI, except for summary health information and enrollment information, are no longer required to comply with the Privacy rule administrative requirements. Due to the nature of self-insured plans, the compliance requirements are quite extensive. Regardless of the compliance requirements, legal review is recommended prior to implementation.

### What are the provisions of the law?

The Privacy Rule defines PHI as any individually identifiable health information pertaining to past, present or future physical or mental health of an individual. PHI identifiers include:

- Names
- Telephone numbers
- Social Security numbers
- Medical Record numbers
- Dates relating to birth, death, admission or discharge

PHI also includes records of provision of care and payment for care such as full medical records, explanation of benefits (EOB) or billing statements.

Under the Privacy Rule, PHI may be used or disclosed only for the following reasons:

- To the individual; and
- For "treatment," "payment," or "health care operations;" and
- In certain cases, to family members or close personal friends if the disclosure relates to health care or payment for care and the individual has been given the opportunity to object.

Other uses and disclosures of PHI require explicit written authorization from the individual. In general, all disclosures pertaining to health information should be limited to the minimum necessary for the purpose of the disclosure.

## Benefit Fact Sheet

### Notice of Privacy Practices

The HIPAA Privacy Rule requires that health plans remind their enrollees about the availability of the Notice of Privacy Practices at least once every 3 years. The reminder only needs to be sent to employees. It is not required to be sent to dependents. The requirement can be met in several ways:

- Send out a copy of the Notice of Privacy Practices.
- Mail a reminder explaining that a Notice of Privacy Practices is available and provide information on how to obtain a copy.
- Include information in a newsletter or in open enrollment materials with the information listed in bullet #2.

### New regulations

The American Recovery and Reinvestment Act (“the Act”; also informally known as the “Stimulus Bill”) signed into law by President Obama on February 17, 2009 contained a section called the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”). The main purpose of the HITECH Act was to further promote electronic communication in the health care area. For example, the HITECH Act promotes the use of “electronic health records” of individuals, in an effort to move away from a paper-based health care system.

The Act also requires business associates to comply directly with many of HIPAA’s rules and subjects business associates to HIPAA’s civil and criminal penalties. The Act increased the penalties for various HIPAA violations and dramatically expanded other remedial actions (such as increasing federal government audits; granting attorneys fees in some HIPAA lawsuits; and allowing a method for individuals to recover penalties under HIPAA). The changes are significant to all covered entities, which now indirectly includes employers as sponsors of Group Health Plans (ERISA plans).

The HITECH Act also made changes to the HIPAA Privacy and Security Rules and have varying effective dates, including the following:

- Increased penalties
- New breach notification rules
- New restriction request rules
- Certain rules relating to electronic health records
- New prohibitions on sale of protected health information (“PHI”)

### Informational link(s)

- [Summary of the HIPAA Privacy Rule](#) (U.S. Department of Health & Human Services)
- [The Department of Health & Human Services’ Health Information Privacy Rights](#)
- [ArlenGroup’s HIPAA Fact Sheet](#) (ArlenGroup)
- [Centers for Medicare and Medicaid Services](#)
- [Health Information Technology for Economic and Clinical Health \(HITECH\) Act](#) (Congressional Research Service)

This Fact Sheet is designed to provide a general overview of the benefit program, service, or regulatory act it describes. The information included in this document is not a substitute for legal or professional opinion relative to a plan sponsor’s particular fact pattern. Your ArlenGroup consultant can answer more specific questions relative to its application for your organization. A menu of additional topics is available online at: [www.arlengroup.com/facts](http://www.arlengroup.com/facts).