Q&A

Legal Compliance

Courtesy of The Reschini Group

Q **Who is governed by the HIPAA Privacy Rule?**

A The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule applies to covered entities. Covered entities include:

- Health plans
- Health care clearinghouses
- Health care providers that conduct certain transactions electronically

The HIPAA Privacy Rule does not directly regulate an employer sponsoring a group health plan; only the health plan is directly regulated. However, where the plan sponsor has access to protected health information (PHI) related to the administration of the health plan, it must comply with the requirements of the HIPAA Privacy Rule. A plan sponsor's access to enrollment applications and disenrollment information alone does not qualify as having access to PHI for the purposes of the rules.

Self-administered, self-funded group health plans with fewer than 50 participants are **not** required to comply with the HIPAA Privacy Rule. In addition, the following benefits are not subject to the HIPAA Privacy Rule:

- Accident-only
- Disability income
- Liability insurance
- Life insurance
- Workers' compensation

Many aspects of the HIPAA Privacy Rule apply directly to business associates. A business associate is an entity or person that performs a function or activity for a covered entity or provides certain services for a covered entity and has access to PHI. The HIPAA Privacy Rule requires covered entities and business associates to enter into an agreement regarding the protection of PHI. The HIPAA Privacy Rule also specifies the provisions that must be contained within a business associate agreement.

THE RESCHINI GROUP®