What Business Associates Must Do:

Business Associates are required under the HIPAA Rules and HITECH (Health Information Technology for Economic and Clinical Health) Act to:

- Comply with the HIPAA Security Rule provisions requiring the implementation of administrative, physical and technical safeguards for electronic PHI, including designating a Security Official, developing related policies and procedures, and training staff;
- Execute and comply with Business Associate Agreements;
- Execute agreements with subcontractors (those persons or entities to whom the Business Associate delegates a function, activity or service, other than in the capacity of a workforce member of the business associate);
- Respond immediately to potential violations and report breaches to the covered entity (McLaren);
- Comply with patient rights under HIPAA, including the rights of access, amendment and accounting of disclosures;
- Comply with those state or federal laws that are more restrictive than the HIPAA requirements;
- Limit the use and disclosure of PHI to the minimum amount necessary, except for treatment purposes and other limited exceptions; and
- Cooperate with compliance investigations and/or reviews of the Secretary of Health and Human Services.

Penalties for Non-Compliance

The penalties for violating HIPAA/HITECH Rules vary depending upon the degree of culpability of the Business Associate and/or subcontractor, and can range from $100 to $50,000 per violation.

Where Can I Learn More?

You can learn more at the U.S. Department of Health and Human Services website: www.hhs.gov/hipaa.

For additional questions, please contact the McLaren Corporate Compliance Officer, Dan Gillett at (810) 342-1438, or at Privacy@Mclaren.org.