GUIDELINES FOR BUSINESS ASSOCIATES

HIPAA

A Covered Entity (CE) is required to adhere to rules established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which is a federal law governing:

- The privacy of identifiable health information – referred to as Protected Health Information (PHI) – regardless of the format in which it exists. This includes electronic, written, and verbal information.

- Electronic Data Interchange and Code Set Standards

- Security of Protected Health Information

HIPAA applies to health care providers, health plans, health care clearinghouses, and such third parties that perform services involving PHI or that exchange electronic data on behalf of a CE (referred to as Business Associates). HIPAA has been modified on a number of occasions.

HIPAA Omnibus Rule of 2013

In January 2013, HIPAA was further revised by what is known as the HIPAA Omnibus Rule. The HIPAA Omnibus Rule includes obligations in addition to those that were set forth under HIPAA and the American Recovery & Reinvestment Act of 2009 (ARRA). Further, the HIPAA Omnibus Rule includes changes to the obligations of Business Associates, requiring an amendment to the Covered Entity's Business Associate Agreement.

As a result, the CE has developed the following documentation in order to comply with the HIPAA Omnibus Rule:

- If the Covered Entity negotiated a HIPAA Business Associate Agreement with you prior to September 23, 2013, by continuing to perform services after September 23, 2013, you agree that your Business Associate Agreement is amended to comply with the HIPAA Omnibus Rule Terms and Conditions for Business Associates. A copy of those Terms and Conditions is available on our website

- If you are a new Business Associate after September 23, 2013, your underlying agreement to provide services to the Covered Entity will require you to comply with the HIPAA Omnibus Rule Terms and Conditions for Business Associates. A copy of those Terms and Conditions is available at on our website.

Federal Trade Commission's "Red Flags" Rules

A Covered Entity must also address requirements related to the Federal Trade Commission's (FTC) "Red Flags" Rules. The Rules were issued under the Fair and Accurate Credit Transactions Act (FACTA). The purpose of the Rules is to aid in the prevention, mitigation, and response to incidents of identity theft.

FACTA has been interpreted so that health care providers, such as Covered Entities, are "creditors" and are, therefore, subject to the Rules. The Rules provide that a creditor is responsible for ensuring its service providers are in compliance with the Rules as well.

As a result, to the extent that you have access to any CE information that may be used to commit identity theft (such as names, Social Security numbers, account numbers, and birth dates), you agree to the following:

- You have implemented sufficient precautions (policies and procedures) to prevent, detect, and mitigate identity theft; and

- You have trained your appropriate staff/employees on these policies and procedures as required by the Red Flags Rules.

Detailed information about the HIPAA Privacy Rule may be found on the web site of the U.S. Department of Health and Human Services.