

Re: Amended HIPAA Business Associate Terms and Conditions & Red Flag Rules

To Whom It May Concern:

On February 17, 2009 President Obama signed the American Recovery & Reinvestment Act (the "ARRA"). Subtitle D of the Stimulus Bill is titled "Privacy" ("ARRA Privacy Rule"). The ARRA Privacy Rule includes both privacy and security provisions that require an amendment to the HIPAA Business Associate Terms and Conditions that UPMC has in place with you or your organization.

As a result, UPMC has placed the following documentation on its web site <http://purchasing.upmc.com>:

1. **"Initial Version of UPMC Terms and Conditions for Business Associates"**. These are the terms and conditions that UPMC has required its HIPAA Business Associates to comply with. These terms have historically been available at <http://purchasing.upmc.com>.
2. **"First Amendment to the Business Associate Agreement"**. This amendment has been drafted to specifically modify those terms that UPMC is obligated to change due to the ARRA Privacy Rule. If UPMC negotiated Business Associate terms and conditions with you, this amendment shall modify those terms and conditions.

If we negotiated HIPAA Business Associate terms and conditions, by continuing to perform services after February 17, 2010, you agree to comply with the First Amendment to the Business Associate Agreement.

3. **"ARRA Revised Terms and Conditions for Business Associates"**. These terms consolidate terms from the "UPMC Terms and Conditions for Business Associates" and the "First Amendment to the Business Associate Agreement".

If you either (a) agreed to the UPMC Terms and Conditions for Business Associates or (b) are a new Business Associate, by continuing to perform services after February 17, 2010, you agree to comply with the Revised Terms and Conditions for Business Associates.

The ARRA Privacy Rule also includes a provision that entitles a UPMC patient to an accounting of who electronically accessed the patient's information. This accounting includes staff of business associates. In order for UPMC to comply with this provision, UPMC requires that you maintain logs of the required information. Additionally, under the ARRA Privacy Rule, UPMC is entitled to direct the patient to the business associate for an accounting of access by the business associate staff. To comply with the ARRA Privacy Rule, UPMC is developing a database of its business associates. UPMC intends to make this database available to its patients so that a patient can directly contact the

business associate(s) directly to request an accounting. To ensure that accurate information is provided to the patient, you should ensure that your company's information found at www.upmc.com/businessassociates is accurate. If the information is not correct, you should fill out the web form on the above referenced web page. Additionally, you may use this web form to designate that either you or your company is not a UPMC Business Associate.

For your information, the ARRA Privacy Rule further contains security terms that Business Associates have direct accountability to comply with (see Sec. 13401). As such, I would recommend that you thoroughly review the ARRA Privacy Rule immediately.

You can find the text of the Privacy provisions of the ARRA at:

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.txt.pdf

UPMC must also address the Federal Trade Commission's (FTC) "Red Flags" Rules requirements. 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 UPMC, 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 UPMC 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 Flag Rules.

Thank you in advance for your cooperation and assistance in this matter.

Sincerely,

John P. Houston

Vice President, Privacy and Information Security & Assistant Counsel