Guidelines for Business Associates

HIPAA

UPMC 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 PHI

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 UPMC (referred to as Business Associates). HIPAA has been modified on a number of occasions, as more fully described below.

In order to comply with HIPAA, UPMC developed the "UPMC Terms and Conditions (PDF) for Business Associates" that all of UPMC's Business Associates must adhere to.

American Recovery and Reinvestment Act (2009)

The American Recovery and Reinvestment Act of 2009 (ARRA) included provisions that modify HIPAA. These provisions required, among other things, that UPMC amend the "UPMC Terms and Conditions (PDF) for Business Associates."

As a result, UPMC developed the following documentation:

- "First Amendment to the Business Associate Agreement" (PDF). This amendment modifies those terms that UPMC was required to change due to ARRA. If UPMC negotiated HIPAA Business Associate terms and conditions with you prior to February 17, 2010, this First Amendment modified those 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."
- "ARRA Revised Terms and Conditions for Business Associates" (PDF). These terms consolidated the terms from the "UPMC Terms and Conditions for Business Associates" and the "First Amendment to the Business Associate Agreement." If you were a new Business Associate after February 17, 2010, you agreed to comply with the "ARRA Revised Terms and Conditions for Business Associates."

HIPAA Omnibus Rule (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 ARRA. Further, the HIPAA Omnibus Rule includes changes to the obligations of Business Associates, requiring a Second Amendment to the "UPMC Terms and Conditions for Business Associates."

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

- “Second Amendment to the Business Associate Agreement” (PDF). This amendment modifies those terms that UPMC was required to change due to the HIPAA Omnibus Rule. If UPMC negotiated HIPAA Business Associate terms and conditions (including the “First Amendment to the Business Associate Agreement”) with you prior to September 23, 2013, by continuing to perform services after September 23, 2013, you agree to comply with the “Second Amendment to the Business Associate Agreement.”
- “HIPAA Omnibus Rule Revised Terms and Conditions for Business Associates” (PDF). These terms consolidated the terms from the “UPMC Terms and Conditions for Business Associates,” the “First Amendment to the Business Associate Agreement.” and the “Second Amendment to the Business Associate Agreement.” If you are a new Business Associate after September 23, 2013, you must comply with the “HIPAA Omnibus Rule Revised Terms and Conditions for Business Associates.”

FTC "Red Flag" Rules

UPMC also must address requirements related to the Federal Trade Commission’s (FTC) “Red Flag” 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 UPMC, are “creditors” and are therefore subject to the Rules. The Rules provide that a creditor is responsible for ensuring that 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.

Questions about HIPAA, the ARRA guidelines for business associates or the "Red Flag" Rules should be directed to the Customer Service Group of Supply Chain Management at 412-647-8070. Detailed information about the HIPAA Privacy Rule may be found on the website of the U.S. Department of Health and Human Services.