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"). Title XIII of ARRA is known as the "HITECH Act." The HITECH Act includes both privacy and security provisions that require an amendment to the HIPAA Business Associate Terms and Conditions that The Regional Cancer Center ("RCC") has in place with you or your organization.

RCC has placed the document called "First Amendment to Business Associate Agreement" on its web site http://www.trcc.org. This Amendment has been drafted to specifically modify those terms of your Business Associate Agreement with RCC that are required to be modified due to the HITECH Act. If you continue to perform business associate services for RCC after February 17, 2010, this Amendment shall automatically modify the terms and conditions of your Business Associate Agreement with RCC unless you notify us in writing that you no longer intend to provide business associate services to RCC. The HITECH Act also includes a provision that entitles RCC's patients to an accounting of who electronically accessed their patient information. This accounting includes staff of business associates. In order for RCC to comply with this provision, RCC requires that you maintain logs of the required information. Additionally, under the HITECH Act, RCC is entitled to direct the patient to the business associate for an accounting of access by the business associate staff. To comply with the HITECH Act, RCC is developing a database of its business associates. RCC 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 http://www.trcc.org 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 an RCC Business Associate.

For your information, the HITECH Act 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 HITECH Act immediately.

You can find the text of the HITECH Act at:

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

RCC must also address the Federal Trade Commission's "Red Flags" Rules (the "Red Flag Rules"). The Red Flag Rules were issued under the Fair and Accurate Credit Transactions Act (FACTA). The purpose of the Red Flag 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 RCC are "creditors" and are therefore subject to the Red Flag Rules. The Red Flag Rules provide that a creditor is responsible for ensuring its service providers are in compliance with the Red Flag Rules as well.

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

- 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 Girard
Executive Director
The Regional Cancer Center