vRad®

p 952.595.1100
f 952.942.3361
www.vrad.com

11995 Singletree Lane, Suite 500
Eden Prairie, MN 55344

November 14, 2011

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Dear Sir/Madam:

I am contacting you on behalf of Virtual Radiologic Professionals, LLC ("vRad") regarding a recent vRad security incident. vRad is located in Minnesota and provides radiology interpretations to hospitals across the country by using its contracted radiologists to review radiology scans.

Unfortunately, vRad recently became aware of a security incident involving a laptop computer that was stolen from a vRad employee's car on Friday, October 14, 2011. The employee discovered the laptop was missing on Saturday morning and immediately notified vRad's IT (information technology) department. Some information pertaining to certain vRad patients and physicians was stored on the computer, including limited medical information for some patients and names, addresses and sensitive information such as bank account numbers, social security numbers or credit card numbers of others. The laptop contained information for only **three** New Hampshire residents.

vRad uses "self-encrypting" hard drives, meaning the computers use a technology that prevents an unauthorized person from seeing the information on the computer. Although the employee and the vRad IT department believed the laptop was secured with the encryption technology, vRad discovered that the company-required encryption was not properly configured on this particular computer due to an error in the setup process. The laptop was password protected, and the file that contains personal information is a hidden file with Microsoft-enabled safeguards. We therefore believe that it is extremely unlikely that whoever stole the laptop could access any personal information. However, because the overall level of encryption was not at the highest level that vRad requires, it is possible that an unauthorized person could gain access to that information.

After discovery of the non-encryption issue on Monday, October 17th, vRad immediately launched an audit of the employee's email files and local drive, which also is backed up to vRad's main information system. Due to the amount of data and multiple ways the employee worked with such data as part of her job, conducting a thorough audit and cataloging the data took a few weeks. vRad engaged a third party vendor to assist with this project. **To date, we have no evidence that any information was actually accessed.** If someone accesses the internet using that computer before it is reimaged with a new operating system, vRad will immediately receive a notice and will "wipe" the laptop completely and permanently.

Local law enforcement was promptly notified. vRad is complying with all New Hampshire and federal law requirements, including the HIPAA breach notification requirements, to notify affected persons. vRad will also notify the Department of Health and Human Services, as required by the federal HIPAA statute. We are taking steps to ensure that this situation does not happen again, such as requiring dual sign-off when new laptops are put into service. We also deployed our IT staff immediately to verify each computer is, in fact, encrypted properly.

vRad began notifying affected parties the week of October 24, 2011. Although there is no evidence that any information has been misused, or even accessed, vRad is taking a number of steps to advise and assist affected physicians and patients. We are providing information on credit report and fraud alert services and advising those affected to be vigilant in monitoring accounts and credit reports for evidence of identity theft. vRad has also contracted with LifeLock, Inc. to provide credit monitoring and alerts to affected persons, at vRad's cost.

As a company that values respect for and accountability to patients, vRad deeply regrets that this event occurred. As indicated above, we have taken steps to comply with all applicable state and federal laws, prevent a reoccurrence of the security risk that occurred, and provide necessary support to our patients and physicians.

If you have any questions concerning this matter, you may contact us at (952) 595-1100, or toll-free at 1-800-737-0610. Please ask for me when calling.

Sincerely,

Karen Scott

Karen Scott, Privacy Officer
Virtual Radiologic Corporation