Maimonides
Medical Center

4802 Tenth Avenue
Brooklyn, NY 11219

Tel: 718 283-7019
Fax: 718 283-7180

jleahy@maimonidesmed.org

Joyce A. Leahy
Senior Vice President for Legal Affairs
& General Counsel

Dear Vendor:

Maimonides Medical Center is committed to ensuring that the personal information of its patients is not disclosed inappropriately. This includes not just protected health information but information such as social security numbers and birth dates which can lead to identity theft.

The New York Information Security Breach and Notification Act, which went into effect December 7, 2005, requires any person or business which conducts business in New York State to notify New York residents and the Attorney General's Office of breaches of personal data.

HITECH, a federal law, enacted February 17, 2009, requires Maimonides to provide notification to patients and government agencies following discovery of a breach of unsecured protected health information (PHI) unless a risk assessment demonstrates there is a low probability that the PHI has been compromised.

Maimonides has committed to taking steps to ensure that loss of sensitive data does not occur. Accordingly, Maimonides strongly recommends the following:

1. Personal information such as names, linked with social security numbers and birth dates, as well as protected health information should never be transmitted by e-mail unless the e-mail is encrypted. Thus, it would be inappropriate for employees to e-mail databases to their homes to work on, unless the e-mail is encrypted. Hackers can obtain this information while it is in transit if it is not encrypted.

2. Laptop loss or theft is the most common event leading to identity theft. Employees and independent contractors should be strongly discouraged from loading personal data of patients on laptops and taking it home with them to work on. Laptops have been stolen from cars and from apartments. Encrypted VPN and SSL tunnels are available, for both employees and independent contractors, providing secure access to sensitive data from a remote location. The MIS command center (718) 283-6227) is available to assist in providing access to this technology.

3. Any data on laptops should be encrypted. If data is encrypted, it does not require notifying the individuals involved of the release of the data (unless the encryption key is also stolen). Levels of password protection, while better than nothing, do not obviate the need to notify the patients under the New York State Information Security Breach and Notification Act or the federal HIPAA Breach Notification Rule.

Maimonides is committed to maintaining the security of its patients' personal and health information. Maimonides needs its vendors to understand the importance of these issues.

Please have an appropriate officer sign below indicating your receipt of this notice and return a copy to me for my files.

Thank you for your attention to this matter.

Sincerely yours,

Joyce A. Leahy
Senior Vice President for Legal Affairs
& General Counsel

JAL:tb

H:\LETTERS\Vendor letter - identity theft issue 03 21 2013.doc