

McDermott Will & Emery

Boston Brussels Chicago Düsseldorf Houston London Los Angeles Miami Milan
Munich New York Orange County Rome San Diego Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

Daniel F. Gottlieb
Attorney at Law
dgottlieb@mwe.com
+1 312 984 6471

April 28, 2010

VIA FEDERAL EXPRESS

Maine Office of the Attorney General
6 State House Station
Augusta, Maine 04333

CONSUMER PROTECTION DIVISION
RECEIVED
APR 29 2010
OFFICE OF ATTORNEY GENERAL

Re: Report of Potential Security Breach

Dear Sir/Madame:

We are writing on behalf of our client, Emergency Healthcare Physicians, Ltd. an Illinois medical corporation ("EHP"), to report a potential security breach of our patients' personal information as a result of the theft of computer equipment from our billing service provider, Millennium Medical Management Resources, Inc. ("Millennium"), containing files with patients' names, Social Security numbers, other demographic information, and in some cases, health information and/or driver's license numbers to the Maine Office of the Attorney General pursuant to the Notice of Risk to Personal Data Act. Although we are not aware of any identity theft or other illegal use of our patient's personal information, EHP is voluntarily making this report and notifying the affected patients so that steps can be taken to protect the patients from any misuse of their information. We also enclose a copy of the form of notice to be sent to patients who are Maine residents.

The theft occurred on Saturday, February 27, 2010 as part of a break-in at Millennium's offices in Westmont, Illinois and was discovered by a Millennium employee the following day. Millennium determined that among the items stolen was a portable hard drive containing unencrypted copies of records with health and financial information about patients served in Illinois hospital emergency rooms by EHP physicians from 2003 to 2006. Millennium believes the hard drive contained personally identifiable information about EHP patients, including name, address, phone number, date of birth, and Social Security Number and, in some cases, other information such as diagnosis and/or diagnosis code, types of procedure and/or procedure code, medical record number, account number, driver's license number, and health insurance information. Millennium does not believe the stolen hard drive contained credit/debit account numbers or other financial account information.

Millennium reported the break-in and theft to the Westmont police department, and together with law enforcement, began investigating the matter immediately upon discovery. The investigation is ongoing and we will provide public notice if we learn of any material developments regarding

Maine Office of the Attorney General

April 28, 2010

Page 2 of 2

the stolen personally identifiable health or financial information. Millennium has implemented new and improved technical, physical and administrative security measures to prevent future thefts and security breaches, including encryption of electronic personally identifiable information stored on portable storage devices. Millennium will also take additional steps to further secure patient information. EHP is carefully monitoring these security measures to assure that they meet regulatory requirements and appropriately secure information about its patients.

EHP takes protection of the privacy and security of its patients' information very seriously. On or before April 30, 2010, we will send the enclosed security breach letter to a total of nine (9) affected Maine residents. Our letter advises the individuals to remain vigilant and consider taking the following steps to avoid identity theft: (1) place a fraud alert on their credit files; (2) review their credit reports; (3) monitor their financial and other accounts; and (4) place a security freeze on their credit files. The letter directs a patient to other resources for further information and describes actions to take if the patient suspects that his or her information is being misused. The letter provides a toll-free phone number for patients with questions about the incident. In addition, we will report this security breach to the Office of Civil Rights of the U.S. Department of Health and Human Services on or before April 30, 2010.

EHP does not directly maintain any personal information about its patients. The hospitals at which EHP physicians treat patients maintain the medical, billing and other personal information about the patients and disclose this information directly to Millennium. The hospitals encrypt the information before transmitting to Millennium.

If you have any questions regarding the potential security breach, please do not hesitate to contact me.

Sincerely,



Daniel F. Gottlieb

Enclosure

cc: Brian Kern, M.D.
Ted Patras, M.D.



April 30, 2010

NAME
STREET ADDRESS
SECONDARY ADDRESS
CITY, STATE ZIP

Dear **NAME**:

We are writing to inform you that Emergency Healthcare Physicians, Ltd. ("EHP") was notified on March 1, 2010, that computer equipment containing health and financial information about you and other EHP patients was stolen from its billing service provider, Millennium Medical Management Resources, Inc. ("Millennium"). Although we are not aware of any actual unauthorized access to the information, identity theft or other misuse of your information, we are notifying you to advise you of the incident and steps that you can take to protect yourself from misuse of the information.

Description of the Incident and Information Involved

The theft occurred on Saturday, February 27, 2010 as part of a break-in at Millennium's offices in Westmont, Illinois and was discovered by a Millennium employee the following day. Millennium determined that among the items stolen was a portable hard drive containing unencrypted copies of records with health and financial information about you and other patients served in Illinois hospital emergency rooms by EHP physicians from 2003 to 2006. Millennium believes the hard drive contained personally identifiable information about EHP patients, including name, address, phone number, date of birth, and Social Security Number and, in some cases, other information such as diagnosis and/or diagnosis code, types of procedure and/or procedure code, medical record number, account number, driver's license number, and health insurance information.

How are EHP and Millennium Responding to the Theft?

EHP takes protection of the privacy and security of your information very seriously. We deeply regret that this incident has occurred and apologize for any inconvenience and concern that this incident has caused you.

Millennium reported the break-in and theft to the Westmont police department, and together with law enforcement, began investigating the matter immediately upon discovery. The investigation is ongoing and we will provide public notice if we learn of any material developments regarding the stolen personally identifiable health or financial information. Millennium has implemented new and improved technical, physical and administrative security measures to prevent future thefts and security breaches, including encryption of electronic personally identifiable information stored on portable storage devices. Millennium will also take additional steps to further secure patient information. EHP is carefully monitoring these security measures to assure that they meet regulatory requirements and appropriately secure information about its patients.

We will report this security breach to the Office of Civil Rights of the U.S. Department of Health and Human Services. If you are a resident of Louisiana, Massachusetts, Maine, New Hampshire, New York, or Puerto Rico, we will also notify your state's Attorney General's office or other state agency responsible for receiving reports of security breaches.

What Steps Can You Take to Protect Yourself?

Although we are not aware of any instance of identity theft or other misuse of your personal information as a result of this incident, we advise you to remain vigilant and consider taking the following steps:

(over)

- *Place a Fraud Alert on Your Credit Files.* Call the toll-free numbers of any of the three national credit bureaus (below) to place a fraud alert on your credit reports. The fraud alert can help prevent an identity thief from opening additional accounts in your name or using your information for other purposes. You only need to contact one of the credit bureaus. Once one credit bureau confirms the fraud alert, it will automatically contact the other two credit bureaus to place alerts on the credit reports. There is no charge to place a fraud alert on your credit reports.

| Equifax | Experian | TransUnion |
|--|--|---|
| 1-800-525-6285 | 1-888-EXPERIAN (397-3742) | 1-800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |
| P.O. Box 740241 Atlanta, GA 30374-0241 | P.O. Box 9532 Allen, TX 75013 | Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790 |

- *Review Your Credit Reports.* The credit bureaus will send individuals a free credit report when they set up a fraud alert. It is highly recommended that you order the free credit report from each of the credit bureaus. You should review credit reports carefully for signs of fraud, such as unfamiliar accounts or credit inquiries or other unusual activity. Even if you do not find any suspicious activity on your credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports regularly. Identity thieves sometimes hold victims' information for a period of time before using it or sharing it among a group of thieves at different times.
- *Monitor Your Financial and other Accounts.* We recommend that you closely monitor your account statements and, if you notice any unauthorized activity, promptly contact the creditor.
- *Place a Security Freeze on Your Credit Files.* You may also be eligible to place a security freeze on your credit file with each of the three credit bureaus. A security freeze, which is different from a fraud alert (discussed in the first bullet point above), prohibits credit bureaus from sharing your credit file with any potential creditors without your approval, making it difficult for an identity thief to use your information to open an account or obtain credit. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of requests you make for new loans, charge cards, housing or other accounts or services. Information about how to request a security freeze and the information that you must provide in order to obtain a security freeze is available from the credit bureaus listed above. The credit bureaus typically charge a fee for a credit freeze.
- *Other Resources.* For more information about steps you can take to avoid identity theft, you may contact the FTC by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, on the Internet at www.ftc.gov/idtheft or by phone at 1-877-ID-THEFT (877-438-4338). You may also contact your state Attorney General or other state agency authorized to receive security breach reports.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police department and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You should also file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Clearinghouse, where it will be accessible to law enforcers for their investigations. In some states, you may also file a report with the Attorney General's Office or another state agency.

* * *

EHP takes its confidentiality obligations to you seriously and strives to take all appropriate measures to safeguard your information internally and when it is required to be disclosed to other healthcare providers or its business associates. Please accept our apologies for the inconvenience this incident has caused you. We are taking this incident very seriously and will continue to monitor Millennium's work with law enforcement and will provide public notification if any material developments arise in the matter.

If you have any additional questions, please call us toll free at 1-800-349-0421.

Sincerely,

Emergency Healthcare Physicians, Ltd.