



Saint Vincent Catholic Medical Centers



www.svcmc.org

The Academic
Medical Center of
New York Medical College
in New York City



Office of Legal Affairs
153 West 11th Street
New York, NY 10001
212-604-8824
facsimile 212-356-4990
estclair@svcmcnyc.org

St. Vincent's Hospital
Manhattan

October 15, 2007

St. Vincent's Hospital
Westchester

Bishop Mugavero Center
for Geriatric Care

Holy Family Home

St. Elizabeth Ann's Health
Care & Rehabilitation
Center

Saint Vincent
Catholic Medical Centers
Behavioral Health
Services

Saint Vincent
Catholic Medical Centers
Home Health Care

Saint Vincent
Catholic Medical Centers
Community-Based
Outpatient Services

Pax Christi Hospice

US Family Health Plan
at Saint Vincent NYC

Office of Consumer Protection
Department of Commerce & Consumer Affairs
235 South Beretania Street, Suite 801
Honolulu, HI 96813

To Whom It May Concern:

I am writing to you pursuant to Section 3(f) of Hawaii's Security Breach Notification Act of 2006 (Haw. Rev. Stat. Title 26, ch. 487N), on behalf of Saint Vincents Catholic Medical Centers of New York ("SVCMC"). On June 1, 2007, SVCMC learned that an employee transmitted copies of certain SVCMC databases containing Social Security numbers and other insurance-related information to his home computer. SVCMC promptly reported the incident to law enforcement, who requested that SVCMC delay notifying individuals of this incident pending their investigation. On September 23, the District Attorney's office of the County of New York granted SVCMC permission to proceed with its notifications.

At this time, we believe that the Social Security number of one (1) resident of Hawaii may have been included in the mishandled databases. SVCMC is in the process of notifying this individual, as well as individuals in other states whose personal information may have been included in the mishandled databases, via written letter through first class mail, postage prepaid, or by such other means as authorized by law. Those letters began mailing on October 12, 2007. For a complete description of the content of such notices, a copy of the notice is attached hereto. If you have any questions, please do not hesitate to contact me.

Sincerely,

Elizabeth St. Clair
Senior Vice President
Chief Legal Counsel

Enclosure



Saint Vincent
Catholic Medical
Centers

October 10, 2007

Dear Valued Patient,

I am writing to let you know about a recent incident involving insurance information held by Saint Vincents Catholic Medical Centers of New York ("SVCMC").

On June 1, 2007, SVCMC learned that an employee transmitted copies of certain SVCMC databases containing insurance-related information to his home computer in February, 2007. There is the possibility that this employee may also have disseminated the databases to an individual not currently employed by or associated with SVCMC. The employee in question had authorization to access the databases as part of his job responsibilities; however, he was not authorized to transmit the databases outside the control of the hospital.

At this time, we have no knowledge of any misuse of this information beyond its unauthorized transmission. However, we wanted to inform you about this incident so that you can best determine what steps you would like to take, if any.

Upon the discovery of this security breach, SVCMC promptly reported it to the proper law enforcement authorities, which in turn began an investigation. To avoid any possible interference with its investigation, the Manhattan District Attorney's office requested that SVCMC refrain from notifying individuals whose information may have been involved.

Independently, we engaged outside computer forensic experts to help us determine what information was contained in the databases and the exact nature and scope of the improper transmission of information outside the control of SVCMC. Although the forensics analysis is ongoing, we have found that certain mishandled databases contained insurance-related information concerning current and former patients, including, for example, name, date of birth, SVCMC account number, insurance carrier information, insurance claim information and insurance policy numbers.

We do not believe that any medical information (such as diagnosis, treatment or medications) was included in these databases. Similarly, we do not believe that the databases contained any credit card or bank account numbers. Together with our outside security experts, we will continue to investigate this matter thoroughly.

During our review of this incident, we determined that your insurance information was included in the compromised databases, and that, to the best of our knowledge, your insurance carrier had used all or part of your (or a family member's) Social Security number as part of its system to identify you.

SVCMC has notified your insurance carrier directly about this situation. Your carrier may elect to take measures to prevent unauthorized individuals from filing claims under your policy. We also recommend that you contact your insurer to inquire about any recent claims that have been made using your policy number.

Credit Monitoring Offer and Other Precautionary Measures

Because we have determined that all or part of your Social Security number was included in the compromised databases, SVCMC is offering to assume the cost for one year of credit monitoring. We have arranged for ConsumerInfo.com, Inc., an Experian company, to provide you with this membership at no cost to you. Experian's credit monitoring product is designed to identify and notify you of key changes in your credit reports that may indicate fraudulent activity. Detailed information about the credit monitoring membership is available at <http://partner.consumerinfo.com/svcmc>.

Important Note: Due to New York state law restrictions, identity theft insurance coverage cannot, by law, be offered by Experian to residents of New York. If you are a resident of New York state, please be aware that Experian's credit monitoring products will not include identity theft insurance, but will otherwise provide services as described by Experian.

You have until January 25, 2008, to activate your credit monitoring membership. To activate your membership, visit <http://partner.consumerinfo.com/svcmc> and enter the access code provided on the top of this letter. This web site will provide further instructions for registration. If you are unable to register or receive notifications online, you can instead use this access code to register for the offline version of Experian's credit monitoring service, by calling 1-888-898-0087.

Whether or not you choose to accept our offer of free credit monitoring, there are a number of additional precautions that you may consider:

- **You may periodically request a free credit report.** Every consumer, whether or not their data has been involved in a security breach, can receive one free report every twelve months from each of the three national credit bureaus listed below. You should remain vigilant about suspicious activity and check your credit reports periodically over the next 12 to 36 months.
- **You may place a fraud alert on your credit file.** A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. To place a fraud alert on your credit file, contact one of the three national credit bureaus at the numbers provided below.
- **In some states, you have the right to put a "credit freeze" on your credit file,** so that no new credit can be opened under your credit file without the use of a PIN number that is issued to you when you initiate your credit freeze. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit bureaus below to find out more information.

To order free credit reports from each of the three national credit bureaus, you can call the numbers below, or you can visit their websites for further contact information:

- Equifax (800) 685-1111 www.equifax.com
- Experian (888) 397-3742 www.experian.com
- TransUnion (877) 322-8228 www.transunion.com

You should know that as a precaution, SVCMC will never ask you to provide any sensitive personal information, such as your Social Security number, except when you have placed a call to us, or through written requests mailed to your home or billing address. If you do happen to receive a telephone or e-mail contact with such a request, it is not from SVCMC and you should not provide any such information.

SVCMC takes the privacy and security of your personal information very seriously. While an incident like this is an unfortunate reality in today's world, we are taking appropriate steps to reduce the chance of any future incidents like this at SVCMC. Specifically, we have reviewed the security settings on our computers to prevent the use of unauthorized programs, and installed new, more effective tools to detect any unauthorized software installed on SVCMC workstations. We are also updating the roles of key IT security personnel and developing additional strategies to promote a secure data environment at SVCMC. We truly regret that this incident occurred.

If you have additional questions or concerns, please feel free to call us at 1-866-675-3853, or you can read the Frequently Asked Questions (FAQs) that we have posted on our web site at <http://www.svcmc.org>.

Sincerely,

Michael Calder
Senior Vice President