

Health Quest

45 Reade Place, Poughkeepsie, NY 12601

(845) 431-5611
Fax: (845) 437-3022

Florie Munroe, CIA, CPA, CHC
Vice President, Chief Compliance Officer

October 20, 2006

Dear Sirs:

Under date of July 7, 2006 we advised your office of a potential security breach at Vassar Brothers Medical Center (see initial report attached). In response to this event our organization retained Kroll to assist with the investigation and, development of a plan of correction. As a result of computer forensic work completed by the Kroll specialists it was determined that the patient demographic information had not been loaded to the stolen laptop. We have notified the public via the press and our web site of the Kroll findings. Attached for your review is the amended report with a copy of the press release.

I would appreciate your acknowledging receipt of this report and advising me if any further information is needed.

Yours,



Florie Munroe

Health Quest

45 Reade Place, Poughkeepsie, NY 12601

(845) 431-5611

Fax: (845) 437-3022

Florie Munroe, CIA, CPA, CHC
Vice President, Chief Compliance Officer

July 7, 2006

Dear Sirs:

As required under the NYS Information Security Breach and Notification Act we are submitting additional information regarding a security breach at one of our affiliate hospitals, Vassar Brothers Medical Center.

Facts:

On June 25th, at approximately 4:45 pm, Vassar Brothers Medical Center's Emergency Department registration staff became aware that a back-up laptop computer was missing from its mobile cart. Staff initially believed the laptop had been legitimately removed for the purpose of maintenance or relocation. However, by 8:30 am on the following morning, May 26th, staff verified that the laptop was missing and could not be located. At that point, the Supervisor of Registration, following the established procedure, immediately notified Security, Risk Management, the Privacy Officer, the Chief Information Security Officer and the Chief Compliance Officer. The Supervisor then began to investigate what data was contained on the laptop.

Investigation:

The Security Department performed a search of the area and notified both the local City of Poughkeepsie police and the New York State Police. Security also began a systematic review of all security camera tapes in areas adjacent to the location of the laptop. Security also assisted ED Registration with completing the required incident reports.

The Chief Information Security Officer (CISO), working with the ED Supervisor, determined what data was ensconced on the computer's hard drive. They were also able to verify when the laptop was last logged onto the network, and for what purpose.

By 11:00 am on June 26th, VBMC had determined that:

- (1) the laptop had been stolen
- (2) access to the computer was password-protected
- (3) the hard drive contained the Master Patient Index (MPI)
- (4) this MPI contained 257,800 patient demographic files containing patient name, date of birth, social security number, and phone number
- (5) the MPI had been downloaded onto the computer three weeks earlier in preparation of a network "down-time and finally

Vassar Brothers Medical Center • Northern Dutchess Hospital • Putnam Hospital Center • Alamo Ambulance Service, Inc.
Hudson Valley Home Care, Inc. • Wells Manor, Inc. • Northern Dutchess Residential Health Care Facility, Inc.
The Foundation for Vassar Brothers Medical Center • NDH Foundation • Putnam Hospital Center Foundation
VBH Insurance Co., Ltd. • Riverside Diversified Services, Inc. • Riverside Management Services, Inc. • HealthServe, LLC.

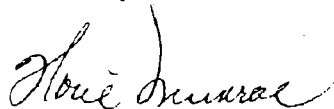
- (6) there was no patient health or diagnostic information on the MPI or on anywhere on the hard drive of the computer

A letter has been drafted to inform these 257,000 individuals that their demographic information was contained on the stolen laptop (see attached). This letter includes steps VBMC has taken to locate the stolen computer, information on contacting the three major credit bureaus and the placement of a "fraud alert" on credit reports, suggestions for preventing identify theft and generally preventing the illicit use of personal information.

VBMC has also contracted with a phone "hotline" company. This company will operate a hotline for concerned individuals with questions about the stolen laptop. The hotline will be available 24 hours a day, 7 days a week for approximately one month. Individuals who have additional questions or concerns will be given the contact information for the Director of Corporate Compliance for Health Quest, the parent non-profit corporation for VBMC.

Please contact me if further information is needed.

Yours truly,



Florie Munroe
Vice President and Chief Compliance Officer
Health Quest

Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
And Notification Act (General Business Law §889-aa;
State Technology Law §208)

Name of Business, Individual or State Entity: Vassar Brothers Medical Center
Date of Discovery of Breach: June 25, 2006
Estimated Number of Affected Individuals: 257,800
Date of Notification to Affected Individuals: July 17, 2006 (estimated mailing date)
Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice. **See Attached**

Please see attached summary of the incident and a copy of the letter to be mailed to each patient
See Attached

Name of Business or Individual Contact Person: Florie Munroe
Title: Vice President ,Chief Compliance Officer
Telephone number: 845 431 5611
Email: fmunroe@health-quest.org

Dated: July 7, 2006
Submitted by: Florie Munroe
Title: Vice President, Chief Compliance Officer, Health Quest
Address: 45 Reade Place, Poughkeepsie, New York 12601
Email: fmunroe@health-quest.org
Telephone: (845) 431-5611 Fax: (845) 483-6870

PoughkeepsieJournal.com Weather Calendar Jobs Cars Real Estate Shopping Classifieds Dating Customer Service

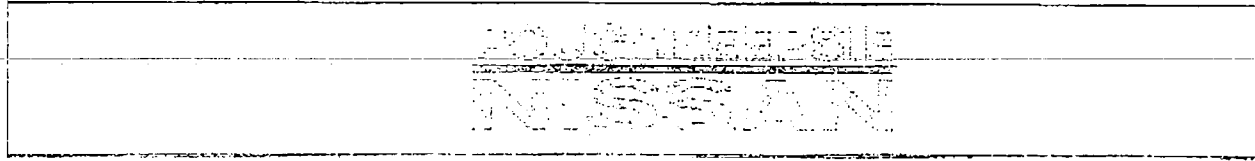


STORY SE

NEWS BUSINESS NATION/WORLD SPORTS OPINION LIFE ENTERTAINMENT VALLEY GUIDE TRAVEL

► IBM in the News ► Ask the Experts ► On the Job ► Young Entrepreneur

ADVERTISEMENT



Thursday, October 5, 2006

Stolen laptop contained no identifying patient information

By Irwin M. Goldberg

e-mail

A private investigation has determined that a laptop taken from Vassar Brothers Medical Center did not contain any personally identifying patient information, center officials said.

Vassar Brothers hired Kroll, an international risk consulting company based in New York City, to investigate the contents of the laptop. Kroll's Web site says it has a division that specializes in computer forensics.

After the theft was discovered in June, the center did its own internal investigation and, based on that, mailed notices to 257,800 patients whose personal data - including Social Security number, address, date of birth and name - officials believed was compromised.

But Kroll's investigation of computer server traffic on the day that patient data - the Master Patient Index - was scheduled to be loaded onto the machines, showed otherwise, a news release issued Thursday night said.

"Kroll was able to go back to computer and server records and determine which were able to connect that day, and it had not connected," said David Ping, vice president of strategic planning and business development for Vassar Brothers, in an interview tonight.

The release said Kroll's investigation determined two laptops didn't connect to the network server that day.

"By comparing serial numbers, IP addresses of the computers and server traffic, Kroll concluded that the MPI information was never loaded onto the laptop that was later stolen," the release said.

For more information, read tomorrow's Poughkeepsie Journal.

To e-mail this article just enter the following information:

*Your name:

*Your e-mail address:



ADVERTI



Related ne Latest head
• Personal F
• Social Sec

Powered by I

Vassar Brothers Medical Center Press Release
October 5, 2006

Poughkeepsie, NY – October 5, 2006 -- Following an extensive investigation by the City of Poughkeepsie Police Department into the theft of a laptop from Vassar Brothers Medical Center and an investigation by Kroll, an independent investigative firm, into the contents of that laptop, Kroll determined that the laptop did not contain any identifying patient information, including names and social security numbers.

The outside cybersecurity and investigation firm Kroll, retained by Vassar Brothers, conducted an extensive and sophisticated analysis of the laptop computers and computer server traffic on the day the Master Patient Index (MPI), which contained names, addresses, date of birth, and social security numbers, was to be uploaded to computers. The Kroll investigation, including extensive interviews, concluded that two laptops did not connect to the network server that day. By comparing serial numbers, IP addresses of the computers, and server traffic, Kroll concluded that the MPI information was never loaded onto the laptop that was later stolen.

VBMC notified the appropriate agencies and sent letters to 257,800 former patients informing them that their information was on the stolen laptop. During the Kroll investigation, VBMC inventoried and secured all copies of patient information, including electronic and paper-based records. Kroll and the City of Poughkeepsie Police met several times over the past six weeks to share findings based on the investigation that they respectively had been conducting.

Janet Ready, Senior Vice President and Chief Operating Officer of VBMC praised the efforts of the City of Poughkeepsie Police, "They have devoted extensive resources to this investigation. We appreciate their tireless efforts to resolve this incident."

Dr. Daniel Z. Aronzon, FAAP, President and CEO of VBMC, said, "We are very sorry this incident took place. We know that this has been stressful for our patients and wanted to let them know as soon as possible that their personnel information was not on the laptop based on a complete and thorough investigation. We put our patients first and conscientiously informed the public of the potential data theft. We have worked with TransUnion to provide special fraud coverage and have been honest and transparent in informing the public of what we knew at that time. For patients who are still concerned about potential identity theft, we have worked with TransUnion to maintain the seven-year fraud alert service. The helpline will also continue to be available from 8:00 a.m. to 4:30 p.m., Monday through Friday. That number is 845-483-6990. We thank the community for its continued support of Vassar Brothers and want our patients to know that we have instituted many changes in our security since this incident occurred."

Vassar Brothers Medical Center retained Kroll in August to complete an independent investigation. As a result we identified ways that the medical Center could improve its physical and cyber security systems. Some of these changes include:

- The MPI is no longer on laptop computers. If the information is needed as a back up or in the event of an emergency, a HealthServe employee will physically take

Vassar Brothers Medical Center Press Release
October 5, 2006

the information from the data center, which has 24 hour security and staffing, to the area

- Encryption software has been purchased and is being installed on laptops
- Security systems and cameras are being upgraded

The hospital is making other changes as well.

A police spokesman said, "The City of Poughkeepsie Police Department is actively investigating the theft of the laptop from Vassar Hospital. Anyone with information on the theft of the laptop is asked to call the City of Poughkeepsie Police at 451-4000. All calls will be kept confidential."

August 4, 2006

People concerned their personal information may have been accessed following the theft of a laptop from Vassar Brothers Medical Center inundated a call center fielding inquiries, hospital officials said.

"They were overwhelmed with the number of calls today," Dave Ping, vice president for strategic planning and business development, said during a conference call with the Journal Thursday.

Calls and e-mails to the Journal from people who received letters about the incident from the hospital indicated long waits for an answer or no answer at all.

The center's phone system was also overwhelmed.

"Calls were coming in at an unbelievable rate," center spokeswoman Jeanine Agnolet said.

A laptop containing personally identifying information of 257,800 patients was stolen from the center in late June.

Officials said additional measures were being put in place overnight to help those affected.

Additional staff members were being brought in to retrieve messages from the voice mail of a hospital staff member, Laura Rosas, whose name and number were listed on the letter sent to affected patients, said Florie Munroe, vice president of compliance at the center.

The letter, in addition to providing information on the theft and what data was taken, recommended patients contact one of the three credit bureaus — Equifax, Experian or Trans Union — and ask that a fraud alert be placed on their credit.

A new hot line was set up, staffed by medical center personnel, said Nick Christiano, chief information officer.

As for recovering the laptop, Detective Lt. William Siegrist said police have reviewed the security videotapes but have no suspects or leads.

If you have information, Siegrist said to call the department at 845-451-4000.

Information can be left anonymously.

Center officials told the Journal Wednesday patient data contained on the laptop dated

to 2000. However, patients who got through to the call center were given different information.

Christiano explained the 2000 date pertained to when the center switched to a new computer system. Data actually dated back about 20 years, he said.

However, that doesn't change the number of patients affected, President and Chief Executive Officer Dr. Daniel Aronson said.

"Patients and former patients were calling in who did not receive a letter concerned about their private information. They don't have to worry," Aronson said, adding everyone who needed to be notified has been sent a letter.

Part of the problem, however, is that some of those affected hadn't received letters until Thursday, some in the morning and some in the afternoon.

Ping said the letters were sent out in batches, the last of which went out last week.

"I want to scream. My information is floating everywhere," said Susan Johnson, who received a letter Thursday. She also received a letter last month from CS Stars after it lost a computer containing personal information on 540,000 New Yorkers.

CS Stars is an independent insurance brokerage working for the Special Funds Conservation Committee, a private agency created under state Workers Compensation law. The committee handles benefits for workers hurt on the job who have had previous injuries.

The computer was later recovered.

"That's what gets me. The information is not protected. I'm getting sick and tired of hearing this," Johnson said. "There has got to be a better way for them to protect our information."

Nancy Fritz of the Town of Poughkeepsie also received a letter from Vassar and CS Stars.

"This is crazy. With all the privacy issues, how can all these computers be taken?" she asked.

Addressing concerns that the laptop was left in a vulnerable place, center officials Thursday clarified that the laptop was secured not only to a mobile cart, but was in a secured room in a restricted area.

"The room is normally locked and the room is secured so the public usually can't get in and medical personnel need a card," Aronson said.

On Wednesday, officials told the Journal the laptop was used as part of two disaster drills and that is why patient data was stored on it. Thursday, however, Agnolet said there was another reason. The laptop served as the backup database for admissions to the emergency department in case there was an outage.

Process altered

The incident already has prompted changes in the way such information is handled.

Patient information is now kept on a server in a secure location and laptops are locked and secured in data management sites on the medical center's campus, Agnolet said.

The data was not encrypted, he said. But it was password protected.

"You would need to be a high-level, tech-oriented person to get through," he said.

Officials also confirmed they notified all necessary state agencies of the theft. Agnolet gave the Journal copies of fax confirmations indicating Munroe sent the notifications to all the agencies on the evening of July 7.

The state Consumer Protection Board indicated in Thursday's Journal it had not received a report.

After realizing there was a lengthy phone tree to wade through, Vassar Brothers decided to provide help to those who want it.

"We've downloaded the standard reporting form for fraud alerts and reproduced it," Munroe said. "We will mail it, with a pre-addressed envelope so all they have to do is fill it out and drop it in the mail."

That form can be obtained by calling the hot line.

"We take this very seriously," Aronson said. "We take the health of the community very seriously and the trust they entrust us with very seriously. We intend to make sure, through various means, that something like this never happens again."

Irwin M. Goldberg can be reached at igoldberg@poughkeepsiejournal.com

Frequently Asked Questions Computer Theft

When was the computer stolen?

The computer was stolen between Friday, June 23 and Monday, June 26, 2006.

Where was it stolen from?

The computer was secured by a cable lock in the emergency department.

How long did it take for VBMC to respond to the theft?

Within 24 hours of the reported theft, we had notified the police and had begun our investigation. Within a week of the theft, we had notified all of the proper authorities and had started our communication with the public.

“Why did it take so long to tell me?”

We needed to verify the names and addresses on the list. This took time, as did the having the letter printed, put in envelopes and sent in the mail. Vassar Brothers did everything possible to get this information to you as quickly as possible.

“I went to Vassar Brothers Medical Center five years ago, why was my name on the computer?”

The Patient Master Index was a computer record of all of Vassar’s patients. We keep the Master Index so patients will receive continuity of care even if there is no electricity or network available. The Index allows the hospital to quickly locate your medical record.

“Why was my information on the computer?”

Vassar Brothers Medical Center was participating in a regional Disaster drill, where the hospital needed to function without the computer network. This incident occurred a week before the theft. In preparation for the drill, the Patient Master Index was downloaded onto the computer.

What information was on the computer?

The computer had demographic information on it – name, sex, phone number, date of birth and social security number.

Was any medical or financial information on the computer?

No. Only demographic information

What are you doing to recover the computer?

We have reported the theft to the local and state police. We are reviewing the security tapes of the area from which the computer was stolen to determine if we can identify a

Frequently Asked Questions Computer Theft

suspect. We continue to cooperate and work diligently with the local authorities in the recovery of the computer

Was my information accessed?

We have no way of knowing if your information was accessed. The computer was password protected. It is our belief and the belief of law enforcement that the computer was stolen because it was a high-end laptop, not because of any information on the computer.

What should I do to protect myself from identity theft?

You should contact one of the three credit bureaus and have them explain their procedures for placing a fraud alert on your credit. The three credit bureaus are:

Experian: 1-888-397-3742

Trans Union: 1-800-680-7289

Do I need to contact all of the credit bureaus?

No. The one that you contact will contact the other two agencies

"I am having difficulty getting through to the credit unions, what do I do?"

The credit unions have generally become full automated and you will probably not be able to contact a "live" person. If you are having difficulty with the voice automated system, you have several options:

1. Have a relative help you call the credit unions
2. Have a relative go online to one of the credit union's websites:
www.experian.com; www.transunion.com;
3. Contact Laura Rosas, Director of Corporate Compliance at 845-838-6454 and leave a message with your address. She will send you a stamped envelope with a form to send to the credit union.

What are you doing to prevent this from happening in the future?

We are reviewing the locations of all of our laptops and the security measures for those computers. We are also considering the encryption of all demographic information.

"Is there someone I can contact for additional information?"

Please contact Laura Rosas, Director of Corporate Compliance and Privacy at Health Quest. Her number is 845-838-6454.

Health Quest

45 Reade Place, Poughkeepsie, NY 12601

(845) 431-5611

Fax: (845) 483-6870

Email: fmunroe@health-quest.org

Florie Munroe, CPA, CHC
Vice President, Compliance

FACSIMILIE TRANSMISSION COVER SHEET

PLEASE DELIVER THE FOLLOWING PAGES TO:

NAME: CPB

DATE: 7-7-06

FAX NUMBER: 518-474-2474

Number of Pages Including Cover Sheet: 6

Comments:

Confidential under NYS Public Health Law 2805-M and/or Education Law 6527(3)

The document(s) accompanying this fax may contain confidential information. It is intended only for the use of the individual to whom it is addressed and may contain information that is privileged and confidential. Federal and State Law prohibit the use or re-disclosure of this information by anyone other than the person listed above.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this telecopied information, except its direct delivery to the intended recipient named above, is strictly prohibited. If you have received this fax in error, please notify us immediately at the telephone number listed above to arrange for the return of the documents to us.

Vassar Brothers Medical Center • Northern Dutchess Hospital • Putnam Hospital Center • Alamo Ambulance Service, Inc.
Hudson Valley Home Care, Inc. • Wells Manor, Inc. • Northern Dutchess Residential Health Care Facility, Inc.
The Foundation for Vassar Brothers Medical Center • NDH Foundation • Putnam Hospital Center Foundation
VBH Insurance Co., Ltd. • Riverside Diversified Services, Inc. • Riverside Management Services, Inc. • HealthServe, LLC.



VASSAR BROTHERS MEDICAL CENTER

July 10, 2006

Dear Patient:

Vassar Brothers Medical Center has recently experienced a theft of one of its laptop computers. This computer was used to register patients in the Emergency Department. The thief had to cut a lock to take the computer. The computer itself was password protected. We are contacting you to inform you that some of your personal information was contained on this computer. The information included your name, date of birth, sex, telephone number and social security number. No medical or financial information was contained on this computer. This theft was promptly reported to both the police and the appropriate state agencies.

However, as a precaution, we are providing you with important information to help you protect and guard against possible identity theft:

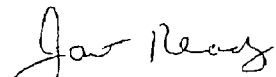
- Call the Credit Bureau – Ask them to explain their procedure for placing a Fraud Alert on your credit. If this procedure and its effect are satisfactory to you, have the Credit Bureau place the alert. The numbers for the credit bureaus are listed below. You do not need to contact all three of these agencies. The agency that you contact will contact the other two agencies:
 - Equifax: 1-800-525-6285
 - Experian: 1-888-397-3742
 - Trans Union: 1-800-680-7289

Fraud alerts last for 90 days. To extend the alert, you must send them a request in writing.

- Be aware of people “phishing” or calling you for information.
 - The type of information that may be requested includes:
 - Bank account information
 - Credit card numbers
 - Pin numbers
 - Legitimate businesses will not call you and ask for this information. In fact, it is their policy to not ask for this. In general, you should not give out this information unless you have initiated the contact.

Although there is no evidence that the hard drive has been inappropriately accessed, we view this matter with the highest degree of concern. Preserving the security of electronic data is a prevalent issue today, with many companies experiencing similar types of incidents. We regret any inconvenience this theft has caused you and want to thank you for your cooperation. To assist you at this time, we have set up a special toll free number for you to call, should you have any additional questions. That number is 1-866-501-2025.

Sincerely,



Janet Ready
Senior Vice President and Chief Operating Officer
Vassar Brothers Medical Center

2 Sources

1-845-483-6990

JAM - 10PM

#2

Health Quest

45 Reade Place, Poughkeepsie, NY 12601

(845) 431-5611

Fax: (845) 483-6870

Email: fmunroe@health-quest.org

Florie Munroe, CPA, CHC
Vice President, Compliance

COPIED

FACSIMILIE TRANSMISSION COVER SHEET

PLEASE DELIVER THE FOLLOWING PAGES TO:

NAME: CPB

DATE: 10-17-06

FAX NUMBER: 518-474-2474

Number of Pages Including Cover Sheet: _____

Comments:

Confidential under NYS Public Health Law 2805-M and/or Education Law 6527(3)
The document(s) accompanying this fax may contain confidential information. It is intended only for the use of the individual to whom it is addressed and may contain information that is privileged and confidential. Federal and State Law prohibit the use or re-disclosure of this information by anyone other than the person listed above.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this telecopied information, except its direct delivery to the intended recipient named above, is strictly prohibited. If you have received this fax in error, please notify us immediately at the telephone number listed above to arrange for the return of the documents to us.

Vassar Brothers Medical Center • Northern Dutchess Hospital • Putnam Hospital Center • Alamo Ambulance Service, Inc.
Hudson Valley Home Care, Inc. • Wells Manor, Inc. • Northern Dutchess Residential Health Care Facility, Inc.
The Foundation for Vassar Brothers Medical Center • NDH Foundation • Putnam Hospital Center Foundation
VBH Insurance Co., Ltd. • Riverside Diversified Services, Inc. • Riverside Management Services, Inc. • HealthServe, LLC.

Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
And Notification Act (General Business Law §889-aa;
State Technology Law §208)


Name of Business, Individual or State Entity: Vassar Brothers Medical Center
Date of Discovery of Breach: _____
Estimated Number of Affected Individuals: ~~257,800~~ None
Date of Notification to Affected Individuals: July 17, 2006 initial;
October 6, 2006 Amended notice
Manner of Notification: written notice/ News paper
 electronic notice (email) Web Site
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice. **See Attached**

Please see attached summary of the incident and a copy of the letter to be mailed to each patient **See Attached**

Name of Business or Individual Contact Person: Florie Munroe
Title: Vice President ,Chief Compliance Officer
Telephone number: 845 431 5611
Email: fmunroe@health-quest.org

Dated: October 20, 2006
Submitted by: Florie Munroe 
Title: Vice President, Chief Compliance Officer, Health Quest _____
Address: 45 Reade Place, Poughkeepsie, New York 12601 _____
Email: fmunroe@health-quest.org _____
Telephone: (845) 431-5611 _____ Fax: (845) 483-6870 _____

Health Quest

45 Reade Place, Poughkeepsie, NY 12601

(845) 431-5611

Fax: (845) 483-6870

Email: fmunroe@health-quest.org

Florie Munroe, CPA, CHC
Vice President, Compliance

FACSIMILIE TRANSMISSION COVER SHEET

PLEASE DELIVER THE FOLLOWING PAGES TO:

NAME: CPB

DATE: 7-7-06

FAX NUMBER: 518-474-2474

Number of Pages Including Cover Sheet: 6

Comments:

Confidential under NYS Public Health Law 2805-M and/or Education Law 6527(3)

The document(s) accompanying this fax may contain confidential information. It is intended only for the use of the individual to whom it is addressed and may contain information that is privileged and confidential. Federal and State Law prohibit the use or re-disclosure of this information by anyone other than the person listed above.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this telecopied information, except its direct delivery to the intended recipient named above, is strictly prohibited. If you have received this fax in error, please notify us immediately at the telephone number listed above to arrange for the return of the documents to us.

Vassar Brothers Medical Center • Northern Dutchess Hospital • Putnam Hospital Center • Alamo Ambulance Service, Inc.
Hudson Valley Home Care, Inc. • Wells Manor, Inc. • Northern Dutchess Residential Health Care Facility, Inc.
The Foundation for Vassar Brothers Medical Center • NDH Foundation • Putnam Hospital Center Foundation
VBH Insurance Co., Ltd. • Riverside Diversified Services, Inc. • Riverside Management Services, Inc. • HealthServe, LLC.

HP Officejet 7210
Personal Printer/Fax/Copier/Scanner

Log for
HQ
845-483-6870
Jul 07 2006 5:55PM

Last Transaction

<u>Date</u>	<u>Time</u>	<u>Type</u>	<u>Identification</u>	<u>Duration</u>	<u>Pages</u>	<u>Result</u>
Jul 7	5:52PM	Fax Sent	915184742474	2:16	6	OK

HP Officejet 7210
Personal Printer/Fax/Copier/Scanner

Log for
HQ
845-483-6870
Jul 07 2006 5:43PM

Last Transaction

<u>Date</u>	<u>Time</u>	<u>Type</u>	<u>Identification</u>	<u>Duration</u>	<u>Pages</u>	<u>Result</u>
Jul 7	5:38PM	Fax Sent	915184742474	5:03	1	Cancel

Health Quest

45 Reade Place, Poughkeepsie, NY 12601

(845) 431-5611
Fax: (845) 437-3022

Florie Munroe, CIA, CPA, CHC
Vice President, Chief Compliance Officer

July 7, 2006

Dear Sirs:

As required under the NYS Information Security Breach and Notification Act we are submitting additional information regarding a security breach at one of our affiliate hospitals, Vassar Brothers Medical Center.

Facts:

On June 25th, at approximately 4:45 pm, Vassar Brothers Medical Center's Emergency Department registration staff became aware that a back-up laptop computer was missing from its mobile cart. Staff initially believed the laptop had been legitimately removed for the purpose of maintenance or relocation. However, by 8:30 am on the following morning, May 26th, staff verified that the laptop was missing and could not be located. At that point, the Supervisor of Registration, following the established procedure, immediately notified Security, Risk Management, the Privacy Officer, the Chief Information Security Officer and the Chief Compliance Officer. The Supervisor then began to investigate what data was contained on the laptop.

Investigation:

The Security Department performed a search of the area and notified both the local City of Poughkeepsie police and the New York State Police. Security also began a systematic review of all security camera tapes in areas adjacent to the location of the laptop. Security also assisted ED Registration with completing the required incident reports.

The Chief Information Security Officer (CISO), working with the ED Supervisor, determined what data was ensconced on the computer's hard drive. They were also able to verify when the laptop was last logged onto the network, and for what purpose.

By 11:00 am on June 26th, VBMC had determined that:

- (1) the laptop had been stolen
- (2) access to the computer was password-protected
- (3) the hard drive contained the Master Patient Index (MPI)
- (4) this MPI contained 257,800 patient demographic files containing patient name, date of birth, social security number, and phone number
- (5) the MPI had been downloaded onto the computer three weeks earlier in preparation of a network "down-time and finally

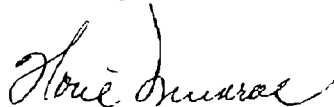
- (6) there was no patient health or diagnostic information on the MPI or on anywhere on the hard drive of the computer

A letter has been drafted to inform these 257,000 individuals that their demographic information was contained on the stolen laptop (see attached). This letter includes steps VBMC has taken to locate the stolen computer, information on contacting the three major credit bureaus and the placement of a "fraud alert" on credit reports, suggestions for preventing identify theft and generally preventing the illicit use of personal information.

VBMC has also contracted with a phone "hotline" company. This company will operate a hotline for concerned individuals with questions about the stolen laptop. The hotline will be available 24 hours a day, 7 days a week for approximately one month. Individuals who have additional questions or concerns will be given the contact information for the Director of Corporate Compliance for Health Quest, the parent non-profit corporation for VBMC.

Please contact me if further information is needed.

Yours truly,



Florie Munroe
Vice President and Chief Compliance Officer
Health Quest