

C	H	O	A	T	E
---	---	---	---	---	---

CHOATE HALL &amp; STEWART LLP

**Fax**

Recipient	Company	Fax	Phone
Linda Conte, Office of Consumer Protection	ME Office of the Attorney General	(207) 626-8812	
<b>From</b>	David N. Sontag	<b>Number of Pages</b>	7
<b>Date</b>	July 19, 2010	<b>Client Number</b>	0699690-0057
<b>Phone</b>	617-248-4729	<b>Operator</b>	<b>Time Sent</b>

**Comments**

Return by      Hold for Pick-up      Inter Office-Mail

This Message is transmitted to you by the law firm of Choate, Hall & Stewart LLP. The substance of this message, along with any attachments, may be confidential and legally privileged. If you are not the designated recipient of this message, please destroy it and notify the sender of the error by return e-mail or by calling 1-800-520-2427.

Under regulations of the Treasury Department, we are required to include the following statement in this message: Any advice contained herein (or in any attachment hereto) regarding federal tax matters was not intended or written by the sender to be used, and it cannot be used by any taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer.

For more information about Choate, Hall & Stewart LLP, please visit us at [www.choate.com](http://www.choate.com)

Two International Place | Boston MA 02110 | t 617-248-5000 | f 617-248-4000 | [choate.com](http://choate.com)



**South Shore  
Hospital**

55 Fogg Road  
South Weymouth  
Massachusetts  
02190-2455  
southshorehospital.org

(781) 340-8000

July 19, 2010

Facsimile: (207) 626-8812

Office of the Attorney General  
Office of Consumer Protection  
6 State House Station  
Augusta, ME 04333

Attention: Ms. Linda Conte

Dear Ms. Conte:

I write to you on behalf of South Shore Hospital in Weymouth, Massachusetts to notify you of the potential loss of certain personal information contained on back-up computer files which affects some of your states' residents. Please note that we have no evidence that the information on the back-up computer files has been accessed by anyone; special software, hardware, and technical knowledge would be required to access and decipher the information. Additionally, the search continues for the missing back-up computer files.

Under HIPAA and the HITECH Act, we are required to issue a notice to appropriate media outlets in your state, which will be issued shortly. We also plan to notify the affected individuals in your state via individual written letters (to be sent by first class mail), although it will take some weeks before those notices can be mailed. In the interim, a form of the individual notification letter that satisfies HIPAA/HITECH requirements and outlines steps potentially affected individuals can take to protect themselves is being posted to the hospital's website at [www.southshorehospital.org](http://www.southshorehospital.org). Additionally, we are establishing a toll-free Information Line to answer frequently asked questions (FAQs), which may be used by all individuals who believe that their information may be at risk as a result of this matter. That line can be accessed by calling (877) 309-0176.

Please see the enclosed documents, which provide additional information about this issue. The first document is the notice that will be issued to local media, as required by HIPAA and the HITECH Act. The second document is a sample individual notification letter that is being posted to the hospital's website. If you have questions or require additional information, please contact me at South Shore Hospital at (781) 624-8432 or [Karen\\_Baxter@sshosp.org](mailto:Karen_Baxter@sshosp.org).

Sincerely,

A handwritten signature in cursive script that reads "Karen Baxter".

Karen Baxter  
Risk Manager  
South Shore Hospital

Encls.

4700004v1



**South Shore  
Hospital**

55 Fogg Road  
South Weymouth  
Massachusetts  
02190-2455  
southshorehospital.org

(781) 624-8000

For release: July 19, 2010

Media Contact: Sarah Darcy, (781) 624-8970

## **SOUTH SHORE HOSPITAL REPORTS POTENTIAL LOSS OF BACK-UP COMPUTER FILES**

South Weymouth, Mass. – South Shore Hospital today reported that back-up computer files containing personal, health and financial information may have been lost by a professional data management company. The hospital had engaged the company to destroy the files because they were in a format the hospital no longer uses. The hospital has no evidence that information on the back-up computer files has been accessed by anyone. An independent information-security consulting firm has confirmed that specialized software, hardware, and technical knowledge and skill would be required to access and decipher information on the files.

Based upon South Shore Hospital's investigation so far, the back-up computer files could contain personally identifiable information for approximately 800,000 individuals. Included among those individuals are patients who received medical services at South Shore Hospital – as well as employees, physicians, volunteers, donors, vendors and other business partners associated with South Shore Hospital – between January 1, 1996 and January 6, 2010. The information on the back-up computer files may include individuals' full names, addresses, phone numbers, dates of birth, Social Security numbers, driver's license numbers, medical record numbers, patient numbers, health plan information, dates of service, protected health information including diagnoses and treatments relating to certain hospital and home health care visits, and other personal information. Bank account information and credit card numbers for a very small subset of individuals also may have been on the back-up computer files.

South Shore Hospital's back-up computer files were shipped for offsite destruction on February 26, 2010. When certificates of destruction were not provided to the hospital in a timely manner, the hospital pressed the data management company for an explanation. South Shore Hospital was finally informed on June 17, 2010 that only a portion of the shipped back-up computer files had been received and destroyed.

South Shore Hospital immediately launched an investigation when it learned that its back-up computer files may have been lost. The investigation has included working with the data management company and shippers to search for the missing back-up computer files, taking steps to verify the scope and types of information contained in the back up computer files, and assessing the possibility that someone could access that information. South Shore Hospital has advised the MA Attorney General's office, the MA Department of Public Health, and the US Department of Health and Human Services about this matter. The hospital also has ceased the offsite destruction of back-up computer files and is putting in place policies to ensure that a similar situation cannot occur. The investigation into the matter remains ongoing.

"I am deeply sorry that these files may have been lost," said Richard H. Aubut, South Shore Hospital president and chief executive officer. "Safeguarding confidentiality is fundamental to our mission of healing, caring and comforting. I recognize that this situation is unacceptable and would like to personally apologize to all those who have trusted us with their sensitive information."

South Shore Hospital is working to verify whose information may have been on the missing back-up computer files. Formal notification letters will be sent to them in the next several weeks. In the meantime, a sample individual notification letter has been posted to the hospital's website at [www.southshorehospital.org](http://www.southshorehospital.org). While there is no evidence that information on the back-up computer files has been improperly accessed, individuals may take steps to protect themselves, such as obtaining a free credit report, which can be done by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or calling (877) 322-8228 toll free, or placing a fraud alert on their credit report with one of the three major credit reporting agencies (Equifax, Experian and TransUnionCorp).

Information about this matter is posted to South Shore Hospital's website at [www.southshorehospital.org](http://www.southshorehospital.org) and is available through a special automated toll-free Information Line at (877) 309-0176.

###



**South Shore  
Hospital**

55 Fogg Road  
South Weymouth  
Massachusetts  
02190-2455  
southshorehospital.org

(781) 624-8000

**SAMPLE LETTER TO INDIVIDUALS WHOSE INFORMATION  
MAY HAVE BEEN ON THE LOST BACK-UP COMPUTER FILES**

Date

Name

Address

City, State

It is with deep regret that I inform you about a serious matter that involves information that you have entrusted to us. A professional data management firm that South Shore Hospital engaged to destroy confidential back-up computer files may have lost them. The back-up computer files may have contained some of your personal, health and financial information.

Based upon our investigation so far, the back-up computer files which are presently unaccounted for may contain protected health information or other personally identifiable information for individuals who received medical services at South Shore Hospital – as well as employees, physicians, volunteers, donors, vendors and other business partners associated with South Shore Hospital – between January 1, 1996 and January 6, 2010. This information may include individuals' full names, addresses, phone numbers, dates of birth, Social Security numbers, driver's license number, bank account or credit card numbers, medical record numbers, patient numbers, health plan information, dates of service, protected health information including diagnoses and treatments relating to certain hospital and home health care visits, and other personal information.

South Shore Hospital has no evidence that information on the back-up computer files has been accessed by anyone. An independent information-security consulting firm has confirmed that specialized software, hardware, and technical knowledge and skill would be required to access and decipher information on the files. Nevertheless, we are obligated under these circumstances to make you aware of this matter and to inform you of steps you may take to protect yourself.

You may receive more than one copy of this notification, despite steps we have taken to avoid sending you duplicate letters.

**About The Situation**

South Shore Hospital engaged the professional data management company to destroy the back-up computer files because they were in a format the hospital no longer uses and because the hospital does not have onsite facilities to professionally destroy the files.

The back-up computer files were shipped for offsite destruction on February 26, 2010. When certificates of destruction were not provided to the hospital in a timely manner, the hospital pressed the data management company for an explanation. South Shore Hospital was finally informed on June 17, 2010 that only a portion of the shipped back-up computer files had been received and destroyed.

South Shore Hospital immediately launched an investigation when it learned that its back-up computer files may have been lost. The investigation has included working with the data management company and shippers to search for the missing back-up computer files, taking steps to verify the scope and types of information contained in the back up computer files, and assessing the possibility that someone could access that information. In addition, South Shore Hospital has advised the MA Attorney General's office, the MA Department of Public Health, and the US Department of Health and Human Services about this matter.

### Steps You Can Take

You are encouraged to read the information below, and in the enclosed attachment, that outlines steps you may take to protect yourself.

- Some state laws, including those in Massachusetts, allow you to place a security freeze on your credit reports. This would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should be aware, however, that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you up to \$5.00 each time you place, temporarily lift, or permanently remove a security freeze. More detailed instructions on how to place or lift a security freeze on your credit card are attached at the end of this letter and are available at [www.southshorehospital.org](http://www.southshorehospital.org).

- You may also want to place a fraud alert on your credit report. This can help prevent someone from opening additional accounts in your name or changing your existing accounts. You can call any one of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the others will be notified automatically of the alert.
- You may also order a copy of your credit report. You are entitled to receive a free credit report annually from each of the three credit bureaus. Even if you do not find suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports and credit card statements periodically.

Equifax  
800-525-6285

Experian  
888-397-3742

TransUnionCorp  
800-680-7289

- In addition, if you believe that you have been the victim of identity theft, you have the right to file a police report and obtain a copy of it. Many creditors will want the information from the police report before excusing you from paying for any fraudulent charges or debts.

- You may also file a complaint with the Federal Trade Commission at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or at 1-877-ID-THEFT (877-438-4338).
- Under some state laws, including those in Massachusetts, you have the right to obtain a copy of any police report made in connection with this matter.
- If you believe someone else may have used your medical information, you may wish to consider taking additional steps which are outlined on the Federal Trade Commission's website at [www.ftc.gov](http://www.ftc.gov).

South Shore Hospital's investigation into this matter continues and will not end until all reasonable efforts have been exhausted.

Safeguarding confidentiality is fundamental to our mission of healing, caring and comforting. As a result of this situation, we immediately ceased the offsite destruction of back-up computer files and have launched a comprehensive review of our data security vendors and internal data-security policies and procedures.

I recognize that you trust our charity with your sensitive information and I am deeply sorry that this unacceptable situation has occurred.

Sincerely,

Richard H. Aubut  
President and Chief Executive Officer

### Instructions on Placing or Terminating Security Freezes on Your Credit Report

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013

TransUnion Security Freeze  
Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identify theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identify theft;
8. If you are not a victim of identify theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash though the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. They must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to permit the removal or lifting of the security freeze.

To lift a security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password originally provided to you when you placed the security freeze. You also will need to provide the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report to be available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the period of time you have specified.

To remove a security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.