

JOHNS HOPKINS INSTITUTIONS

Government, Community and Public Affairs

Suite 540
901 S. Bond Street
Baltimore MD 21231
443-287-9900 / Fax 443-287-9920

DEPARTMENT NAME

DATE: 2.7.07

TO: New York State Consumer Protection Board

Security Breach Notification

FROM: Johns Hopkins

MESSAGE: Attachments

TOTAL # OF PAGES INCLUDING COVER: 13

CONFIDENTIALITY NOTICE: This message is intended for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential, and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately notify the sender via reply e-mail and delete the message from your system.

^
or phone

**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 The Johns Hopkins University
 Date of Discovery of Breach: January 18, 2007
 Estimated Number of Affected Individuals: 52,000 (total) 1091 (New York)
 Date of Notification to Affected Individuals: February 7, 2007
 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.

Appended.

Name of Business or Individual Contact Person: Charlene Moore Hayes
 Title: V.P. Human Resources
 Telephone number: (410) 516 - 8113
 Email: chayes13@jhu.edu

Dated: February 7, 2007
 Submitted by: Charlene Moore Hayes
 Title: V.P. Human Resources
 Address: The Johns Hopkins University, 617 N. Wyman Park Building, 3400 N. Charles Street, Baltimore, MD 21218
 Email: chayes13@jhu.edu
 Telephone: (410) 516-8113 Fax: (410) 516-7242

PLEASE SUBMIT THIS FORM TO ALL THREE (3) STATE AGENCIES as follows:

Fax this form to:

CPB:

Security Breach Notification-

Fax: 518-474-2474

NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC):

30 South Pearl St.

Floor P2

Albany, NY 12207

Fax: 518-474-9090

and also **Fax & Mail** this form to:

Attorney General:

Asst. Attorney General in Charge

Bureau of Consumer Frauds

120 Broadway - 3rd Floor

New York, NY 10271

Fax: 212-416-6003

JOHNS HOPKINS UNIVERSITY

Human Resources

Office of the Vice President
617N Wyman Park Building
3400 N. Charles Street
Baltimore, MD 21218-2696

Charlene Moore Hayes
Vice President

February 7, 2007

New York State Consumer Protection Board
Security Breach Notification
5 Empire State Plaza, Suite 2101
Albany, New York 12223

Dear New York State Consumer Protection Board:

We write to inform you of a recent security incident. As detailed in the attached notice to potentially affected individuals, The Johns Hopkins University became aware on January 18, that eight backup computer tapes containing sensitive personal information on about 52,000 university employees had not been returned as expected by a contractor that routinely makes microfiche backups of such data. The tapes had been sent to the contractor's Baltimore-area facility on December 21.

An investigation by both the contractor and Johns Hopkins has determined that the tapes never reached the facility. It also concluded that it is highly likely that the tapes were mistakenly left by a courier company hired by the contractor at an intermediate stop, in an area where they were collected as trash and later incinerated. The information was not encrypted.

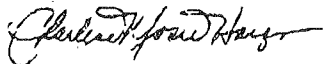
The information on the university payroll tapes included names, Social Security numbers, addresses, bank account information (routing and account numbers), salary, deductions, and retirement plan contributions, for present and former employees. This includes retirees and students who have held campus jobs. Employees whose information is on the tapes come from all university units except the Applied Physics Laboratory.

There is no evidence to indicate that the tapes were stolen or that the data on them has been misused. Johns Hopkins knows of no evidence of identity theft arising from this incident and believes the risk of any such problems is very low. To date, we have received no information, from any source, indicating that the information about any of the potentially affected individuals has been used for any improper purpose.

Johns Hopkins is seeking to notify all affected individuals by sending the attached letter. A Web site has been set up and a toll-free call center has been put in place to provide information about alerting credit reporting agencies. Through our internal investigation following the incident, we have determined that the breach may have affected the personal information of as many as 52,000 individuals, including 1091 residing in New York. We expect our mailing to be complete by mid-February.

Please do not hesitate to contact me at 410-516-8113 should you have questions.

Sincerely,



Charlene Moore Hayes
Vice President for Human Resources
The Johns Hopkins University

Attachment

Dear XXXXXX:

We learned recently that nine backup computer tapes sent out late in December for conversion to microfiche were not returned to Johns Hopkins.

Eight of the nine were payroll tapes containing sensitive, personal information about present and past university employees, including you. The ninth tape contained personal, though less sensitive, demographic information on some Johns Hopkins Hospital patients.

The university tapes included names, Social Security numbers and, for employees paid by direct deposit, bank account information. There was also information on birth dates, salary, deductions and retirement plan contributions.

First, I apologize to you on behalf of the university's entire senior leadership. We do not believe the tapes were stolen or that the information on them has been misused. In fact, the best evidence is that they were inadvertently destroyed. We have no evidence whatsoever of identity theft arising from this incident. Nevertheless, the loss of tapes containing your personal information is, obviously, a situation of significant concern.

An intensive investigation by both Johns Hopkins and the contractor to whom they were sent has determined that the tapes never reached the contractor. We believe that they were mistakenly left at an intermediate stop by a courier hired by the contractor. We believe it is highly likely that they were thought to be trash, collected and incinerated.

WHAT YOU SHOULD DO

Although the best evidence is that the tapes have been destroyed, you may feel it prudent to take precautions. Detailed suggestions are available at <http://www.jhu.edu/identityalert>.

To summarize information available on that Web site: You may request free copies of your credit reports. You also may place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts.

To obtain a free annual credit report, go to <http://www.annualcreditreport.com> or call 877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

To place a fraud alert on your account, call any one of these three major credit bureaus or visit the Experian Web site:

Experian: 800-397-3742 or <http://www.experian.com>

Equifax: 800-525-6285

TransUnionCorp: 800-680-7289

The process is easy and takes just minutes to complete. If you decide to place a fraud alert with any one of the three bureaus, it will notify the others to place alerts on their records as well. Johns Hopkins has notified the three credit bureaus about this situation; they are aware that Johns Hopkins employees may be calling.

There is information on the Web site at <http://www.jhu.edu/identityalert> on what you should do if ever you detect any signs of fraud or other problems in your credit report.

Again, please consult that Web site for more detailed information on this incident. If you do not have access to the Web, we have set up a telephone number for your use. Call 1-800-981-7524.

Please know that people falsely identifying themselves as Johns Hopkins representatives could contact you and offer "assistance." Johns Hopkins will not contact you by phone, mail, e-mail or any other method concerning this incident to ask you for personal information. I urge you not to release personal information in response to contacts of this nature.

The university apologizes to you for this very unfortunate occurrence. I am sure you are concerned. Like you, Johns Hopkins takes this matter very seriously. We will review our processes and procedures and do everything we can to prevent a recurrence. We will post any important new information to the Web site.

Sincerely,

William R. Brody
President
The Johns Hopkins University

**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: The Johns Hopkins Hospital
 Date of Discovery of Breach: January 26, 2007
 Estimated Number of Affected Individuals: 83,000 (total) 767 (New York)
 Date of Notification to Affected Individuals: February 7, 2007
 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.
Appended.

Name of Business or Individual Contact Person: Joanne E. Pollak
 Title: Vice President and General Counsel
 Telephone number: (410) 614-3323
 Email: jpollak@jhmi.edu

Dated: February 7, 2007
 Submitted by: Joanne Pollak
 Title: General Counsel
 Address: 733 North Broadway, BRB 102, Baltimore, MD 21205
 Email: jpollak@jhmi.edu
 Telephone: (410) 614-3322 Fax: (410) 614-3465

PLEASE SUBMIT THIS FORM TO ALL THREE (3) STATE AGENCIES as follows:

Fax this form to:

CPB:

Security Breach Notification-

Fax: 518-474-2474

NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC):

30 South Pearl St.

Floor P2

Albany, NY 12207

Fax: 518-474-9090

and also **Fax & Mail** this form to:

Attorney General:

Asst. Attorney General in Charge

Bureau of Consumer Frauds

120 Broadway - 3rd Floor

New York, NY 10271

Fax: 212-416-6003

**JOHNS HOPKINS**

M E D I C I N E

THE JOHNS HOPKINS
HOSPITAL

Ronald R. Peterson
President
The Johns Hopkins Hospital

February 7, 2007

New York State Consumer Protection Board
Security Breach Notification
5 Empire State Plaza, Suite 2101
Albany, New York 12223

Dear New York State Consumer Protection Board:

We write to inform you of a recent security incident. As detailed in the attached notice to potentially affected individuals, The Johns Hopkins Hospital became aware on January 26, that a backup computer tape containing personal information on approximately 83,000 patients had not been returned as expected by a contractor that routinely makes microfiche backups of such data. The tape had been sent to the contractor's Baltimore-area facility on December 21.

An investigation by both the contractor and Johns Hopkins has determined that the tape never reached the facility. It also concluded that it is highly likely that the tape was mistakenly left by a courier company hired by the contractor at an intermediate stop, in an area where they were collected as trash and later incinerated. The information was not encrypted.

The information on the hospital tape included personal information on all new Johns Hopkins Hospital patients first seen between July 4 and December 18, 2006, or who had changes in their demographic information in that time. The patient information included the patient's name, father's name and mother's maiden name, date of birth, medical history number, race, and gender. It did not include addresses, Social Security numbers, financial information of any kind, or any medical information.

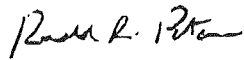
There is no evidence to indicate that the tape was stolen or that the data on it has been misused. Johns Hopkins knows of no evidence of identity theft arising from this incident and believes the risk of any such problems is very low. To date, we have received no information, from any source, indicating that the information about any of the potentially affected individuals has been used for any improper purpose.

New York State Consumer Protection Board
February 6, 2007
Page Two

Johns Hopkins is seeking to notify all affected individuals for whom we have addresses by sending the attached letter. In addition, we are doing outreach to the news media in an effort to reach those for whom we do not have valid addresses. A Web site has been set up and a toll-free call center has been put in place to provide information about alerting credit reporting agencies. Through our internal investigation following the incident, we have determined that the breach may have affected the personal information of as many as 83,000 individuals, including 767 residing in New York. We expect our mailing to be complete by mid-February.

Please do not hesitate to call the General Counsel, Joanne Pollak, at 410-614-3322 should you have questions.

Sincerely,



Ronald R. Peterson
President
The Johns Hopkins Hospital

Attachment

Dear (Patient Name)

We have learned recently that a Johns Hopkins Hospital backup computer tape, sent out in late December for routine transfer to microfiche, was never returned. We believe it is highly likely that it was inadvertently destroyed.

The tape included personal information on more than 83,000 patients of The Johns Hopkins Hospital, all of whom were either new patients first seen between July 4 and December 18, 2006, or who had changes in their demographic information in that time.

Johns Hopkins Medicine faculty and staff, including Johns Hopkins Health System employees, may have been among those patients. We have determined that you are one of the patients.

The important news for you is that the hospital tape included names, mother's maiden name, father's name, race, sex, date of birth and medical record number, but no medical information, Social Security numbers, addresses or financial information of any kind. Moreover, to read the tape requires a sophisticated user and special technology not readily available today. What all of this means is that the risk of identity theft, or other misuse of the information on that tape, is very, very low.

You also should know that because the tape was for backup purposes, none of your information was lost.

We regret this occurrence and emphasize that the best evidence to date is that the tape was not stolen, nor was any information on it misused.

After an intensive investigation by both Johns Hopkins and the contractor to whom the tape was sent, we have concluded that the tape never reached the contractor, and we believe it is highly likely that the tape was thought to be trash, collected as trash, and later incinerated.

While, as we said, the best available evidence suggests that the risk to you is very low, we understand that this situation may be of concern to you, and the leadership of Johns Hopkins has taken several steps to help those who may wish to take precautions.

A Web site has been set up at <http://www.hopkinsmedicine.org/identityalert> with details about what has happened and information about alerting credit reporting agencies. Letters are being sent to all affected Johns Hopkins Hospital patients except those relatively few for whom addresses are unavailable.

Those without access to the Web site can call 1-800-981-7524.

To summarize information available on the Web site: You and all patients may request free copies of credit reports. A fraud alert can be placed on your credit file, which

tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but may also delay you when you seek to obtain credit.

To obtain a free annual credit report, go to <http://www.annualcreditreport.com>, or call 877-322-8228.

To place a fraud alert on your account, patients may call any one of these three major credit bureaus or visit the Experian Web site:

Experian: 800-397-3742 or <http://www.experian.com>

Equifax: 800-525-6285 or <http://www.equifax.com>

TransUnionCorp: 800-680-7289 or <http://www.transunion.com>

As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will then be able to order all three credit reports, free of charge, for your review.

The process is easy and takes just minutes to complete. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Please keep in mind that dishonest people falsely identifying themselves as Johns Hopkins representatives might contact you and offer "assistance." Johns Hopkins will NOT contact patients by telephone, e-mail or any other method to ask for personal information concerning this incident. You should not release any personal information in response to questions of this kind.

We regret this unfortunate event, and stress again that the best evidence to date is that the information on the tape has been destroyed and is highly unlikely to be misused. And we are carefully examining ways to improve our procedures and processes so as to avoid a similar situation in the future.

Very sincerely yours,

Ronald R. Peterson
President
The Johns Hopkins Hospital and Health System