



Ronald R. Peterson  
*President*  
The Johns Hopkins Hospital

February 7, 2007

Kelly A. Ayotte, Esquire  
Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Ms. Ayotte:

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.

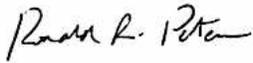
There is no evidence to indicate that the tape was stolen or that the data on it has been misused. Johns Hopkins knows of no evidence of identity theft arising from this incident and believes the risk of any such problems is very low. To date, we have received no information, from any source, indicating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

Kelly A. Ayotte, Esquire  
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 25 residing in New Hampshire. 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



Ronald R. Peterson  
*President*  
The Johns Hopkins Hospital

February 7, 2007

Kelly A. Ayotte, Esquire  
Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Ms. Ayotte:

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.

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 25 residing in New Hampshire. 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