



June 8, 2007

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Dear Sir:

I'm writing to notify you that Concord Hospital recently learned of a serious data security incident that occurred involving personal demographic and health information. On May 30, 2007, Verus Inc. (a third party vendor that Concord Hospital subcontracts with to enable patients to view and pay their bills online) notified us of a lapse that unintentionally occurred in their data security procedures on April 12, 2007. As a result of this lapse, some of Concord Hospital's patient files were left unprotected when the company turned off the firewall, or security device, for maintenance purposes.

The security breach involved a number of files that included 9,297 Concord Hospital patients' and/or guarantors' personal information, including names, dates of birth, addresses and social security numbers. However, no credit card information was exposed and to the best of our knowledge, no one could access personal health information.

Pursuant to RSA 359-C:20, we are notifying you of this breach and also informing you that we've sent direct notification to all the affected patients and guarantors (see attached letter). The personal information was exposed and unprotected on the Internet for over a month before it was discovered, upon which the problem was rectified and the information was immediately secured.

Concord Hospital takes its responsibility to protect our patients' personal information very seriously. Since being notified of the security breach, we have taken all necessary actions to assure our patients' data is secure and we'll do everything we can to prevent this type of breach from occurring again. Please let me know if you require additional information; I can be reached at 227-7000, x3019.

Respectfully submitted,

A handwritten signature in cursive script that reads 'Bruce R. Burns'.

Bruce R. Burns
Sr. VP - Finance/CFO

BRB/kme

Attachment

CONCORD HOSPITAL
IS A CHARITABLE
ORGANIZATION WHICH
EXISTS TO MEET THE
HEALTH NEEDS OF
INDIVIDUALS WITHIN
THE COMMUNITIES
IT SERVES.

June 8, 2007

Dear Concord Hospital Patient:

I am writing to you because we have learned of a serious data security incident that has occurred involving some of your personal information. On May 30, 2007 Verus Inc., the company that Concord Hospital subcontracts with to enable patients to view and pay their bills online, notified us of a lapse that unintentionally occurred in their data security procedures on April 12, 2007. As a result of this lapse, some of Concord Hospital's patient files were left unprotected when the company turned off the firewall, or security device, for maintenance purposes. Data from several other hospitals across the United States was also compromised.

The security breach involved a number of files that included 9,297 Concord Hospital patients and/or guarantors personal information, including name, date of birth, address and social security number. Regrettably, your personal information was included in the data that was at risk. However, **no credit card information was exposed and to the best of our knowledge, no one could access personal health information.**

The personal information was exposed and unprotected on the Internet for over a month before it was discovered, upon which the problem was rectified and the information was immediately secured. We feel it is essential that we notify you of the potential risk.

Concord Hospital takes its responsibility to protect our patients' personal information very seriously. Since being notified of the security breach, we have taken all necessary actions to assure our patient's data is secure and we'll do everything we can to prevent this type of breach from occurring again. In addition we have contacted the New Hampshire Attorney General's Office to alert them of this issue.

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert tells creditors to contact you before they open any new accounts or make changes to your existing accounts. You may activate a fraud alert by contacting any one of the three major credit bureaus below. Once one company has been contacted, the others companies are also notified. You may also consider requesting a free credit report from any of the three companies.

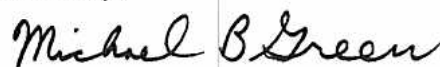
Equifax	Experian	Trans Union
1-800-685-1111	1-888-397-3742	1-800-888-4213
http://www.equifax.com	http://www.experian.com	http://www.transunion.com

If any unusual or suspicious activity is noticed, the FTC recommends you contact the local authorities immediately and file a police report. Additionally, if that should happen, you may also file a report with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

Should you have additional questions or concerns, please contact us. We have established a special telephone line at 603-230-7399 and have dedicated staff available to respond to your needs. You can also check our website, www.concordhospital.org for updated information.

I am truly sorry for any distress that this situation may cause you and all of us at Concord Hospital stand ready to assist in any way that we can.

Sincerely,



Michael B. Green, President/CEO

CONCORD HOSPITAL
IS A CHARITABLE
ORGANIZATION WHICH
EXISTS TO MEET THE
HEALTH NEEDS OF
INDIVIDUALS WITHIN
THE COMMUNITIES
IT SERVES.