

HINMAN STRAUB

ATTORNEYS AT LAW

171 STATE STREET
ALBANY, NEW YORK 12207-1000
TEL: 518-436-0751
FAX: 518-436-4751
E-MAIL: RECEIPTS@HINMAN.COM

*Sean 436-
Doolan 0751
Returning
your call*

CONFIDENTIALITY NOTICE

This document(s) sent to the sender, and intended only recipient, you are hereby notified the contents of this telecopied if please notify us immediately by

confidential, belonging are not the intended y action in reliance on communication in error, is.

**IF THERE ARE ANY PRODU

AT (518) 436-0751

TO: CPB
Security Breach

FROM: Sean Doolan

FAX NO.: 518-474-2474

DATE: March 7, 2007

Number of Sheets (including the cover sheet) 2

COMMENTS:

IRS Circular 230 Disclosure: To comply with Treasury Department Regulations, we are informing you that unless expressly stated otherwise, nothing contained in this document was intended or written to be used, and can not be used or relied upon for the purpose of (1) avoiding penalties imposed under the Internal Revenue Code of 1986, as amended, or (2) promoting, marketing or recommending any tax transaction or matter addressed herein (including attachments).

WELLCHOICE™PO BOX 2107
Church street station
new york, ny 10008-3509
www.wellchoicenj.com

{Group Name}
{Group Contact}
{Address 1}
{Address 2}
{Address 3}
{City} {State} {5-digit zip code}

{Date}

Dear {Group Contact}:

In early February, WellChoice was notified of the loss by UPS of a CD that was sent by a large, national data management company that may contain member personal health and identity information. WellChoice has no indication at this time that the CD was stolen, or that an actual breach of the information has occurred. Both UPS and WellChoice security staff have conducted a thorough search and investigation of the incident and to date the CD has not been found.

It is important to note that you are in receipt of this letter because some members under your current WellChoice group who are or were WellChoice members will receive a letter regarding this shortly if they were impacted. This incident may or may not relate to the member's current health coverage under your group plan as the claims in reference date back to 2003. Because these members may have questions or concerns as a result of this notification, we have established a toll free number for them to call, 800-293-3443, available during the hours of 8:00 am and 7:00 pm eastern time. To ensure that their concerns are addressed appropriately and confidentially, please direct these members to this number to speak with a representative who can provide details specific to their coverage. If you as an employer have questions regarding this incident, please contact your current WellChoice representative for assistance.

We consider the security of our members' personal information a serious matter. We will continue to investigate and monitor this incident and will inform you as soon as possible if we become aware of any new information regarding this matter. As a precaution, WellChoice has made arrangements for free credit watch monitoring over a 12 month period as an option for those who would be more comfortable with this extra measure.

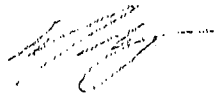
All WellChoice electronic information of this type is required to be encrypted or password protected in transit, including data managed through organizations that contract with us or our customers. By encrypting or password protecting data, WellChoice ensures that the data is unreadable to anyone but the author of the data or by those who have the necessary password to access the information. In this incident, however, Health Data Management Solutions (HDMS), a data manager and third party vendor of one of our benefit program administrators, an independent contractor not affiliated with WellChoice, failed to encrypt or password protect the data. The data may include member or provider names, member social security numbers or member ID numbers and health claims information, including billing codes and service descriptions. We are addressing this issue with the vendor.

Laws and regulations governing potential personal data breaches require investigation and review prior to informing individuals who might be affected. Since being informed of the loss of data, we have been aggressively completing this investigation and review process. We are contacting you and your WellChoice members at the earliest possible point in our review under these requirements.

Shortly we will send a letter to your affected members. In that letter, we will inform them of what happened and offer to them the free credit monitoring for one year through Equifax Credit Watch. I am attaching a copy of that letter for your reference.

We greatly value your business and we are committed to protecting the privacy and security of our members' information. As I commented, we consider the security of our members' personal information a very serious matter and we are committed to protecting their personal and medical information. We believe it is important for you to be fully informed about this situation and we apologize for any inconvenience or concern this may have caused you or your group members. Please be assured that we are taking steps to ensure that this occurrence is not repeated.

Sincerely,



Mark Wagar
President, WellChoice



11 West Forty-Second Street
New York, NY 10036
www.empireblue.com

{First Name} {Last Name}
{Address 1}
{Address 2}
{Address 3}
{City} {State} {5-digit zip code}

{Date}

Dear {Member Name}:

In early February, Empire was notified of the loss by UPS of a CD that was sent by a large, national data management company that may contain your personal health and identity information. Empire has no indication at this time that the CD was stolen, or that an actual breach of the information has occurred. Both UPS and Empire security staff have conducted a thorough search and investigation of the incident and to date the CD has not been found.

We consider the security of our members' personal information a serious matter. We will continue to investigate and monitor this incident and will inform you as soon as possible if we become aware of any new information regarding this matter. As a precaution, Empire has made arrangements for free credit watch monitoring over a 12 month period as an option for those who would be more comfortable with this extra measure.

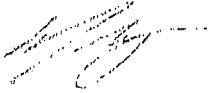
All Empire electronic information of this type is required to be encrypted or password protected in transit, including data managed through organizations that contract with us or our customers. By encrypting or password protecting data, Empire ensures that the data is unreadable to anyone but the author of the data or by those who have the necessary password to access the information. In this incident, however, Health Data Management Solutions (HDMS), a data manager and third party vendor of one of our benefit program administrators, an independent contractor not affiliated with Empire, failed to encrypt or password protect the data. The claims in reference date back to 2003 and may include member or provider names, member social security numbers or member ID numbers, and health claims information including billing codes and service descriptions. We are addressing this issue with the vendor.

Laws and regulations governing potential personal data breaches require investigation and review prior to informing individuals who might be affected. Since being informed of the loss of data, we have been aggressively completing this investigation and review process. We are contacting you at the earliest possible point in our review under these requirements.

To help answer any questions or concerns you may have, we have established a toll free number, 800-293-3443, available during the hours of 8:00 am and 7:00 pm eastern time. You may also begin to receive the free credit monitoring service through Equifax Credit Watch service either by registering online or by mail. To receive notification by mail, please complete the enrollment form we have attached. For online registration, members should visit myservices.equifax.com/gold. This service will monitor your credit file and notify you of any suspicious activity that could indicate potential identity theft. You will need to provide the following promotional code when you enroll, {Promo Code}, and will need to enroll by June 30, 2007. Please also consider taking the steps outlined in the enclosed information sheet to further reduce any potential risk to you.

As I commented, we consider the security of our members' personal information a very serious matter and we are committed to protecting your personal and medical information. We believe it is important for you to be fully informed about this situation and we apologize for any inconvenience or trouble this may have caused you. Please be assured that we are taking steps to ensure that this occurrence is not repeated.

Sincerely,



Mark Wagar
President, Empire BlueCross

Steps you can take to safeguard your personal information

To protect against the misuse of your personal information, you may want to consider placing a security alert on your credit bureau file. If you are enrolling in the credit monitoring service, you may wish to do so before placing the security alert. A security alert marker would cause any issuer of credit to use additional scrutiny for any request for new or increased credit. This provides a significant layer of protection; however, it may limit your ability to get "instant credit" such as the offers often at retail stores. You must contact one of the credit bureaus, below, directly to request this alert.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Some additional precautions that you can take:

- Periodically check your credit report to ensure all your information is correct. To obtain a free credit report once a year, visit www.annualcreditreport.com or call 877.322.8228. Checking your credit reports periodically can help you spot problems and address them quickly.
- If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report as many creditors want the information it contains to absolve you of the fraudulent debts.
- You can also file a complaint with the FTC by contacting them at www.consumer.gov/idtheft, or at 1-877-IDENTTHEFT (438-4338), or at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.

4868X 3/07



121 STATE STREET
ALBANY, NEW YORK 12207-1093
TEL: 518-436-0751
FAX: 518-436-4751
E-MAIL: RECEIPTION@HSPM.COM

FAX TRANSMISSION SHEET

CONFIDENTIALITY NOTICE

This document(s) contained in this facsimile transmission is (are) privileged and confidential, belonging to the sender, and intended only for use by the individual or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking of any action in reliance on the contents of this telecopied information is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone to arrange for the return of the document(s) to us.

**IF THERE ARE ANY PROBLEMS RECEIVING TRANSMISSION, PLEASE CALL AT (518) 436-0751

TO: LISA HARRIS

FROM: SEAN DODD

FAX NO.: 474-2474

DATE:

Number of Sheets [including the cover sheet] _____

COMMENTS:

As discussed!

IRS Circular 230 Disclosure: To comply with Treasury Department Regulations, we are informing you that unless expressly stated otherwise, nothing contained in this document was intended or written to be used, and can not be used or relied upon for the purpose of (1) avoiding penalties imposed under the Internal Revenue Code of 1986, as amended, or (2) promoting, marketing or recommending any tax transaction or matter addressed herein (including attachments).