# THE LOCAL CHOICE E-NEWS

## Department of Human Resource Management
## State and Local Health Benefits Programs

***February 6, 2015***

***Update on Anthem Breach for The Local Choice Members***

The Department of Human Resource Management (DHRM) will provide updates as appropriate to TLC groups on Anthem's recent cyberattack. Scam email campaigns are occurring today regarding credit monitoring related to the Anthem data breach. Please share the attached letter from DHRM and statement with your Anthem members covered by TLC plans. Links to this information are also below.

Thank you for your assistance. As indicated earlier, members should call the Anthem hotline at **1-877-263-7995** with questions about this incident. A special website at **www.anthemfacts.com** will be updated with new information as it is received.

DHRM will continue to monitor the situation and provide updates to TLC groups as necessary. Please let us know if you have questions.

***Please do not reply to this e-mail. You may send inquiries to the Office of Health Benefits mailbox at tlc@dhrm.virginia.gov***

.

# The Local Choice Health Benefits Program

February 6, 2015

Dear The Local Choice Members:

You have probably heard about the Anthem nationwide cyberattack, and we wanted to update you on what the Department of Human Resource Management knows at this time. DHRM takes personal data breaches very seriously. While we know that the data of some Commonwealth of Virginia and The Local Choice members were impacted, Anthem is still investigating the extent of the breach.

Here is what we have been told was taken in the breach for each Anthem member:

- Name
- Home address
- Home phone number
- Home e-mail address
- Date of birth
- Health plan identification number
- Social Security number for some members

Here is what we have been told was NOT taken in the breach:

- Confidential personal health information
- Credit card information

Anthem will notify all members whose information was breached, and will provide credit monitoring and identity protection services free of charge to those affected. Members who have questions may call Anthem's toll-free hotline at **1-877-263-7995** or visit www.anthemfacts.com for updates. A fact sheet and Frequently Asked Questions may be found at http://communique.agencies.virginia.gov/Various/Employee FAQs.pdf and is also attached.

While this is the information we have now, it is subject to change as the investigation continues. If you have additional questions, you may send an email to the DHRM Office of Health Benefits at tlc@dhrm.virginia.gov or call 888-642-4414 or (804) 225-3642 in Richmond.

We will be monitoring the situation closely and will provide updates as appropriate.

Sincerely,

Department of Human Resource Management
State and Local Health Benefits Programs

# Employee Frequently Asked Questions

**Was my information accessed?**

Anthem is currently conducting an extensive IT forensic investigation to determine what members are impacted. The Anthem teams are working around the clock to determine how many people have been impacted and will notify all Anthem members who are impacted through a written communication.

**What information was compromised?**

Anthem's Initial investigation indicates that the member data accessed included names, dates of birth, member health ID numbers, Social Security numbers, addresses, telephone numbers, and email addresses.

**Was there any diagnosis or treatment data exposed?**

No. Anthem's investigation to date indicates there is no evidence that medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

**Was my credit card information accessed?**

No. Anthem's investigation to date indicates there is no evidence that credit card information was compromised.

**Do the people who accessed my information have my Social Security number?**

Yes, in some cases. Anthem is working to determine whose Social Security numbers were accessed.

**How can I sign up for credit monitoring services?**

All impacted members will receive notice via mail which will advise them of the protections being offered to them as well as any next steps.

**When will I receive my letter in the mail?**

Anthem is working to identify the members who are impacted, and expects to mail letters beginning in the next two weeks.

**My children are on my insurance plan, was their information also accessed?**

Yes. Anthem is currently conducting an extensive IT forensic investigation to determine which members are impacted; however, adults and children were impacted.

**Do the people who accessed my information know about my medical history?**

No. Anthem's investigation to date indicates there was no diagnosis or treatment data exposed.

**Do the people who accessed my information have my credit card numbers and banking information?**

No. The investigation to date indicates that information accessed did not include credit card numbers, banking or other financial information.

**Has anyone used my information yet?**

Anthem is not aware of any fraud that has occurred as a result of this incident against its members.

**Am I at risk for identity theft?**

Anthem is currently conducting an extensive IT forensic investigation to determine which members are impacted. Anthem is not aware of any fraud that has occurred as a result of this incident against its members, but all impacted members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

**Do I need a new member ID card and number?**

Anthem will provide further guidance on next steps and we will let you know.

**What is Anthem doing to make my data safe?**

Anthem has contracted with Mandiant – a global company specializing in the investigation and resolution of cyber attacks. Anthem will work with Mandiant to ensure there are no further vulnerabilities and work to strengthen security.

**What is Anthem doing to help members potentially affected by this incident?**

All impacted members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

**Where is the data now? And who can access my information?**

Evidence indicates that the data was uploaded to an external file sharing service. This file sharing service has locked down the account and data so that it cannot be copied, accessed or removed. Anthem and the FBI are working with the file sharing service to access the data and further secure it.

Anthem BlueCross BlueShield

**ANTHEM ALERTS CONSUMERS TO PROTECT THEMSELVES FROM SCAM EMAIL CAMPAIGNS**

Virginia residents who may have been impacted by the cyber attack against Anthem, should be aware of scam email campaigns targeting current and former Anthem members. These scams, designed to capture personal information (known as "phishing") are designed to appear as if they are from Anthem and the emails include a "click here" link for credit monitoring. These emails are NOT from Anthem.

- DO NOT click on any links in email.
- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.
- DO NOT open any attachments that arrive with email.

Anthem is not calling members regarding the cyber attack and is not asking for credit card information or social security numbers over the phone.

This outreach is from scam artists who are trying to trick consumers into sharing personal data. There is no indication that the scam email campaigns are being conducted by those that committed the cyber attack, or that the information accessed in the attack is being used by the scammers.

**Anthem will contact current and former members via mail delivered by the U.S. Postal Service about the cyber attack with specific information on how to enroll in credit monitoring. Affected members will receive free credit monitoring and ID protection services.**

For more guidance on recognizing scam email, please visit the FTC Website: http://www.consumer.ftc.gov/articles/0003-phishing.

For more information on the cyber attack, please visit www.anthemfacts.com.