UNIVERSITY OF NORTH CAROLINA

Date: March 4, 2015

To: UNC State Health Plan Participants

From: **Brian Usischon**
Associate Vice President for Human Resources &
University Benefits Officer

Subject: Anthem Blue Cross Blue Shield Data Breach

You may have heard recently that Anthem Blue Cross and Blue Shield was the target of an external cyber-attack during December 2014 and January 2015. **Systems at Blue Cross and Blue Shield of North Carolina (BCBSNC), which serves as the third party administrator for the State Health Plan, were not breached.** However, approximately 22,000 former and current State Health Plan members who live in or receive care in other Anthem states have been impacted. Anthem operates in the following states: California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin.

If you have been impacted, you will receive an official notice directly from Anthem through the U.S. Postal Service in the next few weeks. The notice will include an offer for two years of free credit monitoring/identity protection services. As additional information becomes available, it will be posted on www.anthemfacts.com.

Information Accessed
The information accessed may have included names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses and employment information, including income data. There is no reason to believe credit card or banking information was compromised, nor is there evidence at this time that medical information such as claims, test results, or diagnostic codes, was targeted or obtained.

Fraudulent E-mail Circulating
You 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 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. For more guidance on recognizing scam emails, please visit the FTC website.

If Your Data Has Been Breached
If you are impacted, you will want to watch for signs of identity theft in the months and years to come. Here are some ways to stay vigilant and protect yourself:

- Monitor your credit. Anthem is offering free credit monitoring and identity protection services to all affected customers. These services will keep an eye on your reports for known indicators of identity theft and send you alerts.

- Sign up for fraud alerts. Contact each of the three major credit bureaus — Experian, TransUnion and Equifax — and ask that a fraud alert be placed on your file.
- Monitor your existing accounts. Watch for unauthorized activity or transfers on your current financial accounts, including 401(k) and brokerage accounts.
- File your tax return as soon as possible.
- Monitor your medical bills. Watch for charges you did not incur.
- Change your bank account PIN.

Employee Assistance Program Resources
For additional resources and tips on dealing with potential identity theft, contact the Employee Assistance Program. Free services are offered through ComPsych and are available 24/7 at http://www.guidanceresources.com/.

Questions?

For more information visit the BCBSNC website or www.anthemfacts.com, or call the Anthem hotline at 877-263-7995.