Anthem Cyber-Attack Information – Updated February 9, 2015

The week of February 2, 2015, EKU was notified of a cyber-security attack on Anthem, our health insurance administrator. Our commitment to you is to provide information as we receive it, to assess the potential exposure for our employees, and to follow up as quickly as possible and as often as necessary to answer everyone's questions.

We are vigilantly monitoring this important situation. Since we first learned of this issue, we have been in contact with both Anthem and Neace Lukens, our insurance consultants. They have pledged to keep us informed as they discover more information about what happened, what impacts there may be on customers, and how they will move forward to mitigate any negative impacts. In addition, an internal EKU team representing Human Resources, IT, and Legal has collaborated and will continue to communicate to ensure that we are providing the most timely information possible, as well as resources for our campus.

Here is what we know at this time:

- Anthem's investigation thus far shows that no credit card or confidential health information (such as claims, test results, or diagnoses) was accessed in this incident.
- The information accessed includes current and former member names, member health ID numbers/Social Security numbers, dates of birth, addresses, telephone numbers, email addresses and employment information, including income data.
- This could include our current and former employees, retirees, and family members who are now or who have been covered under EKU's health insurance at any time in the past.
- Social Security numbers were included in only some of consumer's files that were impacted. Anthem is still working to determine which members' Social Security numbers were accessed.
- There is no indication that any of our employees' personal information has been misused.
- All impacted Anthem members will be enrolled in credit monitoring and identity protection services free of charge. Impacted members will be provided information on how to enroll in free credit monitoring. Anthem will provide that information in a letter mailed directly to affected EKU employees in the next two weeks.
- Anthem has notified the FBI of this cyber-attack, has begun a forensic IT investigation to determine the extent of the breach, has retained one of the world's leading cybersecurity firms to eliminate any further vulnerability, and continues to secure all of its data.

While Anthem is still working to identify what data is impacted, they have made us aware of potential fraudulent e-mails being sent that appear to be from Anthem about credit monitoring services. Kentucky residents who may have been impacted by the cyber-attack against Anthem, which may include current and former EKU employees, should be aware of scam email campaigns targeting current and former Anthem members. These scams, designed to capture personal information (known as "phishing") appear as if they are from Anthem and the emails include a "click here" link for credit monitoring. These emails are **NOT** from Anthem, nor are they from EKU. 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.

Please do not take any action if you receive one of these e-mails.

- DO NOT click on any links in any email you may receive which appears to be from Anthem on this subject.
- 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 the 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. If you receive any calls of this nature, do not give the caller any information and hang up immediately. **Anthem will contact current and former members via mail only, 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.**

Anthem is still working to determine the cause and extent of this cyber-attack. We are continuing to work closely with Anthem to better understand the cyber-attack and the impact on our employees. Additional information about the cyber-attack against Anthem is available at www.AnthemFacts.com. For more guidance on recognizing scam email, please visit the FTC Website: http://www.consumer.ftc.gov/articles/0003-phishing.

We will continue to keep you updated on Anthem's ongoing investigation. In the meantime, HR is available for you at 859-622-5094 or via e-mail at human.resources@eku.edu