**This is confirmation that your memo was just sent to 4,259 email addresses.**

Having trouble viewing this email? Click here.

The University of Arizona
Health Sciences

## Cyber Attack at Banner Health

Banner
University Medical Center

***Below is a message that Banner Health CEO Peter Fine sent to Banner employees earlier today about a massive cyber attack on the Banner computer network. This breach may affect as many as 3.7 million people nationwide, including, perhaps, some at UAHS:***

Dear Colleagues:

Today I regret to inform you of a cyber attack that occurred on Banner's computer network. I want to provide you with the facts about what happened, and what we're doing to help those who may be affected.

**Here are details:**

- On Wednesday, June 29, our IT colleagues detected unusual activity on our computer network.
- We immediately reached out to Mandiant, a leading cyber security firm to help us investigate.
- Working closely with our IT group, Mandiant discovered on July 7 that cyber attackers may have gained unauthorized access to computer systems that process payment card data at the food and beverage outlets at some of our Banner locations.
- We immediately moved to cash-only transactions on a temporary basis to prevent further risk to payment card information and were able to return to accepting all forms of payment at these sites. You can use your payment card with confidence.
- This did not impact payment cards used to pay for medical services.
- We later discovered on July 13 that these same cyber attackers may have also gained access to information on a limited number of servers.
- It is possible that information of approximately 3.7 million individuals may be affected by this incident. Although not all patients are affected by this, there will be employees affected because many are both patients and members of our health plan.
- This information may include name, birthdate, social security number, address, physician names, dates of service, clinical

information and possibly health insurance information if you are a member of a health plan we administer. Further, we know that provider information may be included.
- We have no reports that this information has been misused in any way.

Banner is committed to maintaining the privacy and security of information of our patients, employees, plan members and beneficiaries, customers at our food and beverage outlets, as well as our providers. Today, we are beginning the process of reaching out directly through a letter to all potentially impacted individuals for whom there is contact information. Addresses are being processed through the National Change of Address database. If individuals do not receive a letter by Sept. 9, 2016, but remain concerned that they are affected, they can call the call center number listed below to see if they should have received a letter.

Please be assured that we are working very hard to have resources in place for people affected and to enhance the security around our computer network to help prevent this type of crime in the future.

Unfortunately, cyber attacks on major organizations appear to be on the rise. However, a crime against our organization is also a crime against the individuals affected. It's very personal.

**Here are several free resources to assist those affected:**

- In order to assist you with any questions you may have regarding this incident, we have established a dedicated call center – **1-855-223-4412**. We're asking that employees wait until you receive a notification letter before contacting the call center. If you do not receive a letter by Sept. 9, 2016, but remain concerned that you may be affected, you can call the call center number to see if you should have received a letter.
- We have secured the services of Kroll, a global leader in risk mitigation and response, to provide credit and identity monitoring at no cost to those affected for one year. We have also set up fraud restoration services in the event that anyone experiences fraud. I encourage you to take advantage of these services if you have been affected by this incident.
- We've also created an external website – www.BannerSupports.com -- that contains the same information about the cyber attack. Please refer any patients, visitors, friends and family who may ask about this incident to www.BannerSupports.com so that they, too, can get their questions answered accurately.

I sincerely regret any inconvenience and concern you may experience as a result of this cyber attack. Please know that our internal team and external experts have been working tirelessly to determine the scope of the incident, contain the attack and eliminate it. We are also taking additional steps to further strengthen our computer network and the protections in place for the information we hold.