Banner Health Identifies Cyber Attack

PHOENIX (August 3, 2016) - Banner Health announced today that it is mailing letters to approximately 3.7 million patients, health plan members and beneficiaries, food and beverage customers and physicians and healthcare providers related to a cyber attack. Banner Health immediately launched an investigation, hired a leading forensics firm, took steps to block the cyber attackers and contacted law enforcement.

On July 7, 2016, Banner Health discovered that cyber attackers may have gained unauthorized access to computer systems that process payment card data at food and beverage outlets at some Banner Health locations. The attackers targeted payment card data, including cardholder name, card number, expiration date and internal verification code, as the data was being routed through affected payment processing systems. Payment cards used at food and beverage outlets at certain Banner Health locations during the two-week period between June 23, 2016 and July 7, 2016 may have been affected. The investigation revealed that the attack did not affect payment card payments used to pay for medical services.

On July 13, 2016, Banner Health learned that the cyber attackers may have gained unauthorized access to patient information, health plan member and beneficiary information, as well as information about physician and healthcare providers. The patient and health plan information may have included names, birthdates, addresses, physicians' names, dates of service, claims information, and possibly health insurance information and social security numbers, if provided to Banner Health. The physician and provider information may have included names, addresses, dates of birth, social security numbers and other identifiers they may use. The investigation also revealed that the attack was initiated on June 17, 2016.

This incident did not affect all Banner Health patients.

Banner Health worked quickly to block the attackers and is working to enhance the security of its systems in order to help prevent this from happening in the future. Banner Health is also working with the payment card networks so banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards. Customers should be assured that they can confidently use payment cards at Banner Health food and beverage outlets.

Banner Health is offering a free one-year membership in monitoring services to patients, health plan members, health plan beneficiaries, physicians and healthcare providers, and food and beverage customers who were affected by this incident.

Banner Health encourages its food and beverage customers to remain vigilant to the possibility of fraud by reviewing their payment card statements for any unauthorized activity. These customers should immediately report any unauthorized charges to their card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The telephone number to call is usually on the back of the payment card. Banner Health also recommends that patients review the explanation of benefits statements they receive from their health insurer. If they see any services they did not receive, the patient should contact the insurer immediately.

Banner Health deeply regrets any inconvenience this may have caused. Customers with questions can call 1-855-223-4412, from 7 a.m. to 7 p.m. Pacific Time, seven days a week.

Headquartered in Arizona, Banner Health is one of the largest nonprofit health care systems in the country. The system owns and operates 29 acute-care hospitals, Banner Health Network, Banner – University Medicine, Banner Medical Group, long-term care centers, outpatient surgery centers and an array of other services, including family clinics, home care and hospice services, pharmacies and a nursing registry. Banner Health is in seven states: Alaska, Arizona, California, Colorado, Nebraska, Nevada and Wyoming.

---

http://bannerhealth.mediaroom.com/2016-08-03-Banner-Health-Identifies-Cyber-Attack