Background of Incident and Frequently Asked Questions

Background of security incident

In mid-July Allina Health was notified about a security incident that involved donor and some of our patients' information. The security incident involved a company named Blackbaud, a third-party service provider that provides donor management software to our philanthropic foundations. Blackbaud's fundraising and database services are used by thousands of organizations around the world, including universities, social service nonprofits, health care systems and charitable and philanthropic organizations of all kinds. This was a nationwide incident affecting many organizations so you may have received notices from other nonprofits about this same security incident.

Allina Health began investigating this incident as soon as we received notice of it. In a ransomware attack, cybercriminals attempt to disrupt a business by locking companies out of their own data and servers. After discovering the attack, the Blackbaud Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. However, we have learned that prior to locking down Blackbaud's system, the cybercriminal removed a copy of a subset of non-encrypted data.

Based on the nature of the incident, its own internal research, and a law enforcement investigation, Blackbaud states they have no reason to believe the information was or will be misused. A full description of the incident is available on the Blackbaud website at www.blackbaud.com/securityincident. Blackbaud did pay the cybercriminal's demand with confirmation that the copy of the data that they removed had been destroyed.

What Allina Health is doing to protect personal information

Protecting your information is something we take very seriously. Since learning of this incident, we have been working with Blackbaud to understand the scope of the ransomware attack and the steps it is taking to prevent future data security incidents. Our security experts have evaluated Blackbaud's security protocols and feel confident it has taken the appropriate action to further protect the information entrusted to it.

Frequently Asked Questions:

1. What kind of information was involved?

A very limited amount of information may have been involved.

The information did include:

- Names
- Addresses

This information may have included:
- Dates of birth
- Dates we cared for patients
- The names of doctors who admitted or treated patients
- Allina departments/locations visited

This information **DID NOT** include:
- Credit card information
- Bank account information
- Social security numbers
- Any additional medical information, such as diagnosis or treatment plan

2. Why does Allina Health collect this information? Why was any patient information in this database for your foundations?

As a nonprofit organization, we rely on support from our foundations to help fund the health care services, treatment and research that enables us to provide outstanding care to our patients. Often, people choose to make a donation to a foundation after they or a loved one has a positive experience with us. We, like many other health care organizations, track a limited amount of information in the Blackbaud database so we're able to identify which doctor or department someone has interacted with in case they'd like to direct their gift to a specific program. Programs like this are common among nonprofit health care organizations, and this information is collected to advance the nonprofit mission of Allina Health.

3. Does HIPAA allow this data sharing to Allina Health's foundations?

Yes this is allowed under HIPAA. Allina Health tracks a limited amount of patient information. The information we collect is contact information and limited information such as the dates we cared for patient, doctor names and departments/locations visited.

4. Can I opt out of Fundraising? I do not want the Foundation to contact me in the future.

An individual may choose to opt out of future fundraising communication. Please contact the call center staff with this request by providing your name, phone number and address to Allina_Privacy@intellbc.com.

5. Was my information involved and how can I know?

We have sent communication to individuals whose information may have been involved.

6. Have affected donors and patients been notified?

Allina Health has notified those impacted by this incident. In addition, there is a link to the notice on our website which will be in place for the next 90 days and a press release was sent out to relevant newspapers.

7. What should I do?

We do not believe that this incident puts individuals at risk for identity or financial theft. No financial information was shared. We encourage affected patients to continue practicing the usual caution around suspicious communication, and promptly report any suspected identity theft or other suspicious activity to the proper law enforcement authorities.

8. When did the situation occur?

Allina Health was notified by our vendor in late July and immediately began an investigation. The vendor was impacted in May and conducted an investigation with law enforcement.

9. What measures have been take to prevent this from happening again?

Blackbaud's internal team and external experts have worked to remediate all potential exploitation paths. We have been notified by Blackbaud that the specific system weakness exploited by the cybercriminal has been successfully remediated. Attackers' tactics and tools are constantly evolving; new vulnerabilities are identified every day. Blackbaud and Allina Health employ a team of highly trained and experienced information security professionals to identify and respond to security issues in addition to a 24/7/365 Managed Security Service Provider. The industry standard incident response methodology used by Blackbaud allowed the security team to act quickly and contain the malicious activity. Blackbaud regularly tests its incident response plan and capabilities through recurring incident response tabletop exercises, and they perform regular penetration testing to evaluate their preventative, detective, and responsive security capabilities.

10. I want to file a complaint; where can I do this?

You may file a complaint with the Allina Health Privacy Office by writing to the following address:

Allina Health Privacy Office
Mail Route 10811
P.O. Box 43
Minneapolis, MN 55440-0043

In addition, the federal Office for Civil Rights has been notified of this situation.

If you would like to submit an additional complaint to the Office for Civil rights you can submit your complaint on their website: (http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html), by email OCRComplaint@hhs.gov, or by mail:
Centralized Case Management Operations
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F HHH Bldg.
Washington, D.C. 20201