BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Lynn Sessions
direct dial: 713.646.1352
lsessions@bakerlaw.com

January 18, 2022

VIA E-MAIL: IDTHEFT@OAG.STATE.MD.US

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Ciox Health, LLC ("Ciox"), headquartered in Alpharetta, Georgia, to notify your office of a security incident involving Maryland residents. Ciox is providing this notice on behalf of Essentia Health.[1]

Ciox is a healthcare information management company whose services include processing request for patient medical records. Ciox provides these services for healthcare providers across the United States, including Essentia Health.

On July 2, 2021, Ciox became aware of unusual activity involving one employee's email account. Ciox immediately secured the account and launched an investigation with the assistance of an outside cybersecurity firm. The investigation determined that an unauthorized person accessed the employee's email account between June 24, 2021 and July 2, 2021, and during that time may have downloaded emails and attachments in the account. Because the investigation was unable to determine whether any emails and/or attachments were actually viewed or acquired, Ciox immediately began a comprehensive review of the account's contents to determine whether sensitive information was contained in the account.

On September 24, 2021, Ciox received preliminary results from this review and learned that certain emails and attachments in the employee's email account contained some limited patient information related to our billing and/or other customer service requests. On November 2, 2021,

[1] The notifying entity is a covered entity as defined by the by the Health Insurance Portability & Accountability Act ("HIPAA"), and Ciox is their business associate as defined by HIPAA.

the review was completed and confirmed the full scope of affected individuals and the covered entities to which their information related. Based on this review, Ciox determined that the email account contained names, dates of birth, provider names, medical record numbers and/or date(s) of service for certain patients of healthcare providers for whom Ciox provides services.

After confirming the scope of affected individuals and associated covered entities, Ciox worked to provide notice to applicable healthcare providers. Between November 23, 2021 and January 13, 2022, Ciox notified healthcare providers of this incident. Since then, Ciox has worked with providers to notify the affected individuals whose information was identified by the review.

On January 18, 2022, Ciox began mailing notification letters to affected individuals on behalf of Essentia Health, which includes one Maryland resident, via U.S. First-Class Mail in accordance with HIPAA (45 CFR §§ 160.103 and 164.400 *et seq*.) and Md. Code Ann., Com. Law § 14-3504. A sample copy of the notification letter is enclosed as **Appendix A.** Ciox has also established a dedicated, toll-free call center where all individuals may obtain more information regarding the incident. Ciox also posted notice of the incident on its website.

To help prevent something like this from happening again, Ciox is implementing additional procedures to further strengthen its email security and is providing enhanced cybersecurity training to employees on identifying and avoiding suspicious emails.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Lynn Sessions
Partner

Enclosure

APPENDIX
A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Dear <<first_name>> <<last_name>>:

Ciox Health ("Ciox") contracts with healthcare organizations to provide health information management services. We place a high value on maintaining the privacy and security of the information we maintain for our customers. Regrettably, we are writing to inform you of a security incident that involved some of your information, received in connection with the services Ciox provided for <<b2b_text_1[CE Name]>>. We advised <<b2b_text_1[CE Name]>> of this incident on <<b2b_text_2[Date of notification to CE]>>. While we have no indication that your information has been misused, this letter explains the incident, outlines the measures we have taken in response, and steps you can take.

What Happened? An unauthorized person accessed one Ciox employee's email account between June 24 and July 2, 2021, and during that time may have downloaded emails and attachments in the account. Ciox reviewed the account's contents to determine whether sensitive information was contained in the account. On September 24, 2021, Ciox learned that some emails and attachments in the employee's email account contained limited patient information related to Ciox billing and/or other customer service requests. The review was completed on November 2, 2021 and confirmed that some of your information was contained in the account.

What Information Was Involved? The information involved included your name and provider name<<b2b_text_3[, as well as your [insert other data elements, if any]]>>. Your Social Security number and financial information were **not** included. It is important to note that the Ciox employee whose email account was involved did not have direct access to any healthcare provider's or facility's electronic medical record system.

What We Are Doing. Data privacy and security are among Ciox's highest priorities, and we have extensive measures in place to protect information entrusted to us. To help prevent similar incidents from happening in the future, we are implementing additional procedures to further strengthen our email security and are providing enhanced cybersecurity training to our employees.

What You Can Do. We believe that the account access occurred for the purpose of sending phishing emails to individuals unrelated to Ciox, not to access your information. Still, we wanted to notify you of this incident and assure you we take this very seriously. As a precaution, we recommend you review statements you receive from your healthcare providers and health insurer. If you see charges for services you did not receive, you should contact the provider or insurer immediately.

For More Information. We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at 1-855-618-3107, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Elizabeth A. Delahoussaye, RHIA, CHPS
Chief Privacy Officer

BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Lynn Sessions
direct dial: 713.646.1352
lsessions@bakerlaw.com

January 28, 2022

VIA E-MAIL: IDTHEFT@OAG.STATE.MD.US

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Ciox Health, LLC ("Ciox"), headquartered in Alpharetta, Georgia, to notify your office of a security incident involving Massachusetts residents. Ciox is providing this notice on behalf of the entities identified in **Appendix A**, collectively referred to as the "Notifying Entities" in this notice.[1] This incident was previously reported to your office on January 18, 2022.

Ciox is a healthcare information management company whose services include processing request for patient medical records. Ciox provides these services for healthcare providers across the United States, including the above referenced Notifying Entities.

On July 2, 2021, Ciox became aware of unusual activity involving one employee's email account. Ciox immediately secured the account and launched an investigation with the assistance of an outside cybersecurity firm. The investigation determined that an unauthorized person accessed the employee's email account between June 24, 2021 and July 2, 2021, and during that time may have downloaded emails and attachments in the account. Because the investigation was unable to determine whether any emails and/or attachments were actually viewed or acquired, Ciox immediately began a comprehensive review of the account's contents to determine whether sensitive information was contained in the account.

[1] The notifying entities are covered entities as defined by the by the Health Insurance Portability & Accountability Act ("HIPAA"), and Ciox is their business associate as defined by HIPAA.

On September 24, 2021, Ciox received preliminary results from this review and learned that certain emails and attachments in the employee's email account contained some limited patient information related to our billing and/or other customer service requests. On November 2, 2021, the review was completed and confirmed the full scope of affected individuals and the covered entities to which their information related. Based on this review, Ciox determined that the email account contained names, dates of birth, provider names, and/or date(s) of service for certain patients of healthcare providers for whom Ciox provides services. In limited instances, the information involved may have also included health insurance information, and/or clinical or treatment information.

After confirming the scope of affected individuals and associated covered entities, Ciox worked to provide notice to applicable healthcare providers. Between November 23, 2021 and January 20, 2022, Ciox notified healthcare providers of this incident. Since then, Ciox has worked with providers to notify the affected individuals whose information was identified by the review.

On January 28, 2022, Ciox began mailing additional notification letters to affected individuals on behalf of Notifying Entities, which includes 50 Maryland residents, via U.S. First-Class Mail in accordance with HIPAA (45 CFR §§ 160.103 and 164.400 *et seq*.) and Md. Code Ann., Com. Law § 14-3504. A sample copy of the notification letter is enclosed as **Appendix B.** Ciox has also established a dedicated, toll-free call center where all individuals may obtain more information regarding the incident. Ciox also posted notice of the incident on its website.

To help prevent something like this from happening again, Ciox is implementing additional procedures to further strengthen its email security and is providing enhanced cybersecurity training to employees on identifying and avoiding suspicious emails.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Lynn Sessions
Partner

Enclosures

Appendix A

Notifying Entities:

1. Providence Health System
2. Ascension Seton
3. St. Agnes HealthCare, Inc.

APPENDIX B

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

Dear <<first_name>> <<last_name>>:

Ciox Health ("Ciox") contracts with healthcare organizations to provide health information management services. We place a high value on maintaining the privacy and security of the information we maintain for our customers. Regrettably, we are writing to inform you of a security incident that involved some of your information, received in connection with the services Ciox provided for <<b2b_text_1[CE Name]>>. We advised <<b2b_text_1[CE Name]>> of this incident on <<b2b_text_2[Date of notification to CE]>>. While we have no indication that your information has been misused, this letter explains the incident, outlines the measures we have taken in response, and steps you can take.

What Happened? An unauthorized person accessed one Ciox employee's email account between June 24 and July 2, 2021, and during that time may have downloaded emails and attachments in the account. Ciox reviewed the account's contents to determine whether sensitive information was contained in the account. On September 24, 2021, Ciox learned that some emails and attachments in the employee's email account contained limited patient information related to Ciox billing and/or other customer service requests. The review was completed on November 2, 2021 and confirmed that some of your information was contained in the account.

What Information Was Involved? The information involved included your name and provider name<<b2b_text_3[, as well as your [insert other data elements, if any]]>>. Your Social Security number and financial information were **not** included. It is important to note that the Ciox employee whose email account was involved did not have direct access to any healthcare provider's or facility's electronic medical record system.

What We Are Doing. Data privacy and security are among Ciox's highest priorities, and we have extensive measures in place to protect information entrusted to us. To help prevent similar incidents from happening in the future, we are implementing additional procedures to further strengthen our email security and are providing enhanced cybersecurity training to our employees.

What You Can Do. We believe that the account access occurred for the purpose of sending phishing emails to individuals unrelated to Ciox, not to access your information. Still, we wanted to notify you of this incident and assure you we take this very seriously. As a precaution, we recommend you review statements you receive from your healthcare providers and health insurer. If you see charges for services you did not receive, you should contact the provider or insurer immediately.

For More Information. We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at 1-855-618-3107, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Elizabeth A. Delahoussaye, RHIA, CHPS
Chief Privacy Officer