



55 East Monroe Street
37th Floor
Chicago, IL 60603

312 346 7500 main
312 580 2201 fax
thompsoncoburn.com

Melissa K. Ventrone
312 580 2219 direct
mventrone@thompsoncoburn.com

June 30, 2017

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

RECEIVED

JUL 06 2017

CONSUMER PROTECTION

Dear Attorney General Foster:

We represent PVHS-ICM Employee Health and Wellness LLC ("PVHS-ICM") with respect to a recent security incident involving the potential exposure of certain personally identifiable information described in more detail below. PVHS-ICM operates the UCHealth Walk In Clinic (the "Clinic") in Fort Collins, Colorado.

1. Nature of security incident.

On May 4, 2017, PVHS-ICM discovered that a server in the Clinic containing patient records may have been impacted by ransomware. PVHS-ICM immediately began an internal investigation and hired independent computer forensic experts to assist. The forensic investigation determined that an unauthorized user gained access to the server and infected it with ransomware. There is no evidence that any personal information or protected health information was actually accessed or removed from the server. However, because the server contained information that may have included patient names, addresses, medical records (diagnosis and treatment information), health insurance policy numbers, other demographic information, and in some instances Social Security numbers, PVHS-ICM notified patients out of an abundance of caution.

2. Number of New Hampshire residents affected.

Two (2) New Hampshire residents were notified of the incident. A notification letter was sent to the affected individuals on June 30, 2017 via regular mail, a copy of which is enclosed.

3. Steps you have taken or plan to take relating to the incident.

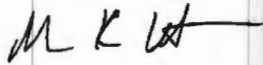
PVHS-ICM has taken steps to prevent this kind of event from happening in the future, including taking the impacted server offline, creating an encrypted backup of the information on the server, and storing the backup in a secure location. Impacted individuals can sign up for 12 months of credit monitoring and identity restoration services through ID Experts. Notice was also provided to the major credit reporting agencies and Health and Human Services Office of Civil Rights.

4. Contact information.

PVHS-ICM remains dedicated to protecting the sensitive information in its systems. If you have any questions or need additional information, please do not hesitate to contact me at MVentrone@ThompsonCoburn.com or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP

A handwritten signature in black ink, appearing to read "M K Ventrone", with a long horizontal flourish extending to the right.

Melissa K. Ventrone

Enclosure

PVHS-ICM Employee Health and Wellness, LLC
C/O ID Experts
PO Box 10444
Dublin, OH 43017-4044

To Enroll, Please Call:
1-866-562-9067
Or Visit:
www.IDExpertsCorp.com/protect
Enrollment Code: [XXXXXXXX]

<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<ZIP>>

<<Date>>

Notice of Security Incident

Dear <<Name>>:

We are writing to inform you of a data security incident experienced by PVHS-ICM Employee Health and Wellness LLC ("PVHS-ICM") that may have resulted in the exposure of your personal information, including your name, Social Security number, and medical information. PVHS-ICM currently operates the UHealth Walk In Clinic at the location formerly utilized by Miramont Urgent Care at 2211 S. College Ave., Fort Collins, CO 80525 (the "Clinic"). This security incident involved a computer server previously utilized by Miramont Urgent Care; the server has not been utilized by PVHS-ICM since September, 2014. This security incident was limited to this single physical location and did not impact any other clinic. We value and respect the privacy of your information, and we sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

1. What happened and what information was involved:

On May 4, 2017, we discovered that a server in the Clinic containing patient records may have been impacted by ransomware. The server contained records for patients seen at the Clinic prior to September 23, 2014. We immediately began an internal investigation and hired independent computer forensic experts to assist us. The forensic investigation determined that an unauthorized user gained access to the server in order to infect it with the ransomware. We have no evidence that any of your personal information was actually accessed or removed from the server. However, because the server contained information that may have included your name, address, Social Security number, medical records (diagnosis and treatment information), health insurance policy number, and other demographic information, we decided to notify you out of an abundance of caution. The server did not contain any financial information. This server was not connected to any other computer systems and did not have information more recent than September 22, 2014.

2. What we are doing and what you can do:

Because we value the privacy and security of your information, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include:

- 12 months of credit and CyberScan monitoring,
- \$1,000,000 insurance reimbursement policy,
- Exclusive educational materials, and
- Fully managed id theft recovery services.

With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-866-562-9067 or going to www.idexpertsCorp.com/protect and using the Enrollment Code provided at the top of this letter. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Mountain Time. Please note the deadline to enroll is 9/30/2017.

We want to assure you that we are taking steps to prevent this kind of event from happening in the future, including taking the server offline, creating an encrypted backup of the information on the server, and storing the backup in a secure location.

3. For more information:

If you have any questions or concerns, please call 1-866-562-9067 Monday through Friday from 6 am - 6 pm Mountain Time. Your trust is a top priority for PVHS-ICM, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

James Sprowell, MD
Manager
PVHS-ICM Employee Health and Wellness LLC

U.S. State Notification Requirements

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 105139
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland, Illinois, North Carolina, and Rhode Island:

You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Attorney General

Consumer Protection Div.
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Attorney

General
Consumer Protection Div.
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Attorney

General
Consumer Protection Div.
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue,
NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identityTheft.gov

For residents of Massachusetts:

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022

www.equifax.com

<http://www.experian.com/freeze>

www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.