Fisher Broyles

December 15, 2023

Via Email (attorneygeneral@doj.nh.gov)

Office of the Attorney General
State of New Hampshire
1 Granite Place South
Concord, NH 03301

Re: CompleteCare Health Network - Notice of Data Security Incident

To Whom it May Concern:

The undersigned represents CompleteCare Health Network ("CCHN"), a non-profit, federally qualified entity that provides primary medical, dental and counseling services to underprivileged constitutes throughout New Jersey, specifically in Cumberland, Gloucester, and Cape May Counties. CCHN was recently the victim of a sophisticated ransomware incident in which an unauthorized third party accessed some of CCHN's computer systems. On behalf of CCHN, we write to provide you notice of the incident and inform you that New Hampshire residents were impacted. This letter also explains the steps that have been taken to address the incident.

What Happened? On October 12, 2023, CCHN detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed some of CCHN's computer systems. CCHN immediately disconnected the affected systems, secured its network environment, and engaged third-party forensic specialists to assist with investigating the extent of any unauthorized activity.

What Information was Impacted? CCHN determined that personal and patient health certain

As of this writing, CCHN has not received any reports of fraud or identity theft related to this disclosure.

Upon further examination, CCHN determined that the incident may have resulted in the exposure of information pertaining to approximately 15 New Hampshire residents. CCHN mailed notification letters to all affected individuals on December 15, 2023, via First Class Mail. Sample copies of the letters sent to these residents are attached for your review as **Exhibit A**.

Steps CCHN has taken. Immediately upon discovery of the incident, CCHN secured its networks by taking the affected systems offline, implemented measures to confirm the security of its systems, engaged with a third-party forensic firm to assist in investigating the extent of the

unauthorized activity and safely restored its systems and operations via viable backups. CCHN also promptly notified the Federal Bureau of Investigation ("FBI") and has worked cooperatively with the FBI's investigation into this cyber-attack.

CCHN has taken steps to further secure its network our network and mitigate the risk of a similar incident occurring in the future, including revising its policies and procedures and network security software, and revising how it stores and manages data. Additionally, CCHN's network environment has been under 24/7 monitoring by cybersecurity experts to mitigate the chance of a future incident, and they have engaged leading cybersecurity firms to assist with monitoring their network for the long term.

Moreover, CCHN notified the following entities beginning on or around December 15, 2023: the U.S. Department of Health and Human Services' Office for Civil Rights (OCR); certain state Attorneys General; prominent media outlets in New Jersey pursuant to 45 CFR § 164.406; and the consumer reporting agencies.

As noted above, CCHN will begin notifying impacted individuals on or around December 15, 2023. Impacted individuals will receive written notice pursuant to the enclosed notification letter template. Certain individuals will also receive substitute notice through the CCHN's website at https://completecarenj.org/about-completecare-nj/notice-of-cybersecurity-incident/.

For more information: Please do not hesitate to contact us if you have any questions regarding this letter.

Respectfully Submitted,
/s/ Maryam Meseha
MARYAM M. MESEHA, ESQ.
on behalf of FisherBroyles, LLP

CompleteCare Health Network
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted] RT 77
ELMER, NJ 08318

December 7, 2023

Notice of Data Incident

SI DESEA RECIBIR ESTE AVISO EN ESPAÑOL, POR FAVOR MARQUE 856-451-4700, OPCIÓN 7. GRACIAS.

Dear [redacted]:

CompleteCare Health Network (CCHN) is a non-profit, federally qualified entity that provides primary medical, dental, and counseling services to underprivileged constituents throughout New Jersey, specifically in Cumberland, Gloucester, and Cape May Counties.

We are writing to inform you of an incident that may have exposed your protected health information and personal information. We take the security of your information seriously and want to provide you with information and resources you can use to protect your information.

At present, there is no evidence that any of your personal information has been misused; however, out of an abundance of caution, we are notifying you of this incident and offering you the resources discussed below so that you can take precautionary steps to protect yourself, should you wish to do so.

What Happened

On or around October 12, 2023, we detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed some of CompleteCare's computer systems. We immediately disconnected the affected systems, initiated our response protocols and engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity, including whether any patient information was accessed.

Our investigation determined that the unauthorized third party may have acquired your personal data during this incident. Please know that we have taken steps to ensure your data will not be further published or distributed. We have also notified, and are working with, federal law enforcement to investigate.

While we have found no evidence that your information has been misused, we are notifying you of this incident and offering you the resources below in an abundance of caution and so that you can take precautionary steps to protect yourself, should you wish to do so.

What Information Was Involved

At present, there is no evidence that any of your personal information has been misused; however, the impacted data may have contained your personal information, including your

What We Are Doing

Data security is one of our highest priorities. As discussed above, upon discovering the incident we immediately took the affected systems offline and began the process of securing and confirming the fortification of our systems. We engaged third-party forensic specialists to confirm the security of our network and investigate the extent of the incident. We also notified federal law enforcement.

We have taken steps to further secure our network and mitigate the risk of a similar incident occurring in the future, including revising our policies and procedures and network security software, and revising how we store and manage data. Additionally, our network environment has been under 24/7 monitoring by cybersecurity experts to mitigate the chance of a future incident, and we have engaged leading cybersecurity firms to assist with monitoring our network for the long term.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau.

Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/completecare** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Steps

In addition to enrolling in the complimentary identity theft protection services being offered, we encourage you to review the enclosed *Additional Important Information* for additional information on how to protect against identify theft and fraud.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 6:00 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at 856-451-4700, press option 7 and supply the fraud specialist with your unique code listed above.

On behalf of CompleteCare, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of protected health information and personal information that we maintain and understand the frustration, concern, and inconvenience that this incident may have caused. I can assure you that we are taking steps intended to prevent an incident like this from reoccurring and to protect you and your information, now and in the future.

Sincerely,

James Edwards, President & CEO
CompleteCare Health Network

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: 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 from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.A

For Residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

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, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: 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 by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

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 make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
equifax.com/personal/credit-report-services/	experian.com/freeze/center.html	transunion.com/credit-freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

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