



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 29, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Continuum Health Alliance, LLC (“Continuum”) located at 402 Lippincott Drive, Marlton, NJ 08053, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one hundred seventy-four (174) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Continuum does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 19, 2023, Continuum discovered suspicious activity within its network. In response, Continuum immediately took steps to secure its systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in Continuum’s network between October 18, 2023 and October 19, 2023, and accessed and acquired certain files stored on those systems during this time. Continuum identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, this extensive review was completed, and Continuum confirmed the extent of information involved. Since that time, Continuum has worked to verify the information and locate missing addresses in order to provide an accurate notice.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, financial account information, medical information, health insurance information, and passport number.

Notice to Maryland Residents

On February 16, 2024, Continuum posted notice of this incident on its website, while the data review process was still ongoing, in order to begin providing notice to those who may be affected. On April 29, 2024, Continuum provided written notice of this incident to one hundred seventy-four (174) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Continuum moved quickly to investigate and respond to the incident, assess the security of Continuum systems, and identify potentially affected individuals. Further, Continuum notified federal law enforcement regarding the event. Continuum is also working to implement additional safeguards and training to its employees. Continuum is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose Social Security number was potentially affected by this incident, at no cost to these individuals.

Additionally, Continuum is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Continuum is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Continuum is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Continuum is also notifying the U.S. Department of Health and Human Services, and prominent media in relevant states pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/ljw
Enclosure

EXHIBIT A



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Date>>

<<City>>, <<State>> <<Zip>>

<<Country>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

Continuum Health ("Continuum") is providing notice of an event that impacts the privacy of some of your personal information. We are in possession of your information because we are a provider of health management and patient care coordination services to healthcare organizations, including your health insurer. Continuum takes this incident very seriously, and we are providing information about the incident, our response to it, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On October 19, 2023, Continuum discovered suspicious activity within our network. In response, we immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in our network between October 18, 2023 and October 19, 2023, and accessed or acquired certain files stored on those systems during this time. We identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, this extensive review was completed, and we confirmed the extent of information involved. Throughout this review process, Continuum coordinated efforts with the health insurers involved and worked to locate missing address information in order to provide an accurate notice.

What Information Was Involved? Our review determined that the following types of information were present in the files that were accessed and acquired by the unauthorized actor: your name, [data elements]. Although the investigation was unable to confirm whether your information was actually viewed by the unauthorized actor, we are unable to rule out this possibility. Please note that Continuum is not aware of actual or attempted fraudulent misuse of any individual's information as a result of this event.

What We Are Doing. The confidentiality, privacy, and security of personal information is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. Federal law enforcement is aware of this incident, and we also notified applicable regulators as required, including the U.S. Department of Health and Human Services.

Additionally, as an added precaution, we are offering you credit monitoring and identity theft protection services for [12/24] months through TransUnion, at no cost to you. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. If you have additional questions or need assistance, please call our dedicated assistance line at [XXX-XXX-XXX] between the hours of [X:00 a.m. to X:00 p.m.] Eastern time, Monday through Friday, excluding all major U.S. holidays. You may also write to Continuum at 404 Lippincott Drive, Marlton, New Jersey 08053.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Continuum Health

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <<URL>> and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [X] Rhode Island residents that may be impacted by this event.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 30, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Continuum Health Alliance, LLC (“Continuum”) located at 402 Lippincott Drive, Marlton, NJ 08053, and are writing to supplement our April 29, 2024 notice to your office. By providing this notice, Continuum does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 19, 2023, Continuum discovered suspicious activity within its network. In response, Continuum immediately took steps to secure its systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in Continuum’s network between October 18, 2023 and October 19, 2023, and accessed and acquired certain files stored on those systems during this time. Continuum identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, Continuum concluded its extensive review of the impacted data and determined that personal information was contained within the files. Since this time, Continuum has worked to coordinate efforts with the health plans involved that own the data at issue and located missing address information in order to provide an accurate notice.

The information that could have been subject to unauthorized access includes name, medical information, and health insurance information.

Notice to Maryland Residents

On February 16, 2024, Continuum posted notice of this incident on its website, while the data review process was still ongoing, in order to begin providing notice to those who may be affected. On April 29, 2024, Continuum began mailing notice letters to impacted individuals. On May 30, 2024, Continuum provided written notice of this incident to thirty-two (32) additional Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. As such, notice was provided to two hundred six (206) total Maryland residents.

Other Steps Taken and To Be Taken

Upon discovering the event, Continuum moved quickly to investigate and respond to the incident, assess the security of Continuum systems, and identify potentially affected individuals. Further, Continuum notified federal law enforcement regarding the event. Continuum is also working to implement additional safeguards and training to its employees. Continuum is providing access to credit monitoring services for 1 year, through TransUnion, to individuals whose Social Security number was potentially affected by this incident, at no cost to these individuals.

Additionally, Continuum is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Continuum is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Continuum is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Continuum is also notifying the U.S. Department of Health and Human Services and prominent media in relevant states pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/ljw
Enclosure

EXHIBIT A



May 30, 2024

NOTICE OF DATA BREACH

Dear :

Continuum Health (“Continuum”) is providing notice of an event that impacts the privacy of some of your personal information. We are in possession of your information because we are a provider of health management and patient care coordination services to healthcare organizations, including your health plan. Continuum takes this incident very seriously, and we are providing information about the incident, our response to it, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On October 19, 2023, Continuum discovered suspicious activity within our network. In response, we immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in our network between October 18, 2023 and October 19, 2023, and accessed or acquired certain files stored on those systems during this time. We identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, Continuum concluded its extensive review of the impacted data and determined that information related to you was contained within the files. Since this time, Continuum has worked to coordinate efforts with the health plans involved and located missing address information in order to provide you with an accurate notice.

What Information Was Involved? Our review determined that the following types of information were present in the files that were accessed and acquired by the unauthorized actor: your name, date of birth, payor, diagnosis/clinical information, geographic subdivisions, health insurance policy-related number, medical dates of services, medical provider name, medical treatment/procedure information, other patient identifier, and telephone numbers. **The information disclosed did not include Social Security numbers or financial information.** Although the investigation was unable to confirm whether your information was actually viewed by the unauthorized actor, we are unable to rule out this possibility. Please note that Continuum is not aware of actual or attempted fraudulent misuse of any individual’s information as a result of this event.

What We Are Doing. The confidentiality, privacy, and security of personal information is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. Federal law enforcement is aware of this incident, and we also notified applicable regulators as required, including the U.S. Department of Health and Human Services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information. If you have additional questions or need assistance, please call our dedicated assistance line at 1-833-961-7515 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding all major U.S. holidays. You may also write to Continuum at 404 Lippincott Drive, Marlton, New Jersey 08053.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Continuum Health

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1- year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094



Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 25, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Continuum Health Alliance, LLC (“Continuum”) located at 402 Lippincott Drive, Marlton, NJ 08053, and are writing to supplement our May 30, 2024 notice to your office. By providing this notice, Continuum does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 19, 2023, Continuum discovered suspicious activity within its network. In response, Continuum immediately took steps to secure its systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in Continuum’s network between October 18, 2023 and October 19, 2023, and accessed and acquired certain files stored on those systems during this time. Continuum identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, Continuum concluded its extensive review of the impacted data and determined that personal information was contained within the files. Since this time, Continuum has worked to coordinate efforts with the health plans involved that own the data at issue and located missing address information in order to provide an accurate notice.

The information that could have been subject to unauthorized access includes name, medical information, and health insurance information.

Notice to Maryland Residents

On February 16, 2024, Continuum posted notice of this incident on its website, while the data review process was still ongoing, in order to begin providing notice to those who may be affected. On April 29, 2024, Continuum began mailing notice letters to impacted individuals. On June 25, 2024, Continuum provided written notice of this incident to two (2) additional Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. As such, notice was provided to two hundred six (208) total Maryland residents.

Other Steps Taken and To Be Taken

Upon discovering the event, Continuum moved quickly to investigate and respond to the incident, assess the security of Continuum systems, and identify potentially affected individuals. Further, Continuum notified federal law enforcement regarding the event. Continuum is also working to implement additional safeguards and training to its employees. Continuum is providing access to credit monitoring services for 1 year, through TransUnion, to individuals whose Social Security number was potentially affected by this incident, at no cost to these individuals.

Additionally, Continuum is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Continuum is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Continuum is providing written notice of this incident to relevant state and federal regulators, as necessary. Continuum also notified the U.S. Department of Health and Human Services and prominent media in relevant states pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/ljw
Enclosure

EXHIBIT A



June 25, 2024

NOTICE OF SECURITY INCIDENT

Continuum Health (“Continuum”) is providing notice of an event that impacts the privacy of some of your personal information. We are in possession of your information because we are a provider of health management and patient care coordination services to healthcare organizations, including your health plan. Continuum takes this incident very seriously, and we are providing information about the incident, our response to it, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On October 19, 2023, Continuum discovered suspicious activity within our network. In response, we immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in our network between October 18, 2023 and October 19, 2023, and accessed or acquired certain files stored on those systems during this time. We identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, Continuum concluded its extensive review of the impacted data and determined that information related to you was contained within the files. Since this time, Continuum has worked to coordinate efforts with the health plans involved and located missing address information in order to provide you with an accurate notice.

What Information Was Involved? Our review determined that the following types of information were present in the files that were accessed and acquired by the unauthorized actor: your name, date of birth, diagnosis/clinical information, geographic subdivisions, health insurance policy-related number, medical dates of services, medical provider name, medical record number, and payor. **The information disclosed did not include Social Security numbers or financial information.** Although the investigation was unable to confirm whether your information was actually viewed by the unauthorized actor, we are unable to rule out this possibility. Please note that Continuum is not aware of actual or attempted fraudulent misuse of any individual’s information as a result of this event.

What We Are Doing. The confidentiality, privacy, and security of personal information is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. Federal law enforcement is aware of this incident, and we also notified applicable regulators as required, including the U.S. Department of Health and Human Services.

000010102G0500

P

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information. If you have additional questions or need assistance, please call our dedicated assistance line at 1-833-961-7515 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding all major U.S. holidays. You may also write to Continuum at 404 Lippincott Drive, Marlton, New Jersey 08053.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Continuum Health

Steps You Can Take To Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094



Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft you also have the right to file a police report and obtain a copy of it.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 21, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We continue to represent Continuum Health Alliance, LLC (“Continuum”) located at 402 Lippincott Drive, Marlton, NJ 08053, and are writing to supplement our April 30, 2024 notice to your office. By providing this notice, Continuum does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 19, 2023, Continuum discovered suspicious activity within its network. In response, Continuum immediately took steps to secure its systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in Continuum’s network between October 18, 2023 and October 19, 2023, and accessed and acquired certain files stored on those systems during this time. Continuum identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On March 8, 2024, Continuum concluded its extensive review of the impacted data and determined that personal information was contained within the files. Since this time, Continuum has worked to validate the information and locate missing addresses in order to provide an accurate notice.

The information that could have been subject to unauthorized access includes name, Social Security number, health insurance information, and medical information.

Notice to Maryland Residents

On February 16, 2024, Continuum posted notice of this incident on its website, while the data review process was still ongoing, in order to begin providing notice to those who may be affected. On April 29, 2024, Continuum began mailing notice letters to impacted individuals. On August 21, 2024, Continuum provided written notice of this incident to two hundred one (201) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Continuum moved quickly to investigate and respond to the incident, assess the security of Continuum systems, and identify potentially affected individuals. Further, Continuum notified federal law enforcement regarding the event. Continuum is also working to implement additional safeguards and training to its employees.

Additionally, Continuum is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Continuum is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Continuum is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Continuum is also notifying the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/ljw
Enclosure

EXHIBIT A



August 21, 2024

NOTICE OF SECURITY INCIDENT

Dear

Continuum Health (“Continuum”) is providing notice of an event that impacts the privacy of some of your personal information. We are in possession of your information because we are a provider of health management and patient care coordination services to healthcare organizations, including your health plan or health insurer. Continuum takes this incident very seriously, and we are providing information about the incident, our response to it, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On October 19, 2023, Continuum discovered suspicious activity within our network. In response, we immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party industry specialists. The investigation determined that an unauthorized actor gained access to certain systems in our network between October 18, 2023 and October 19, 2023, and accessed or acquired certain files stored on those systems during this time. We identified the affected files and conducted a comprehensive review of the files in order to identify the type of information contained therein, and to whom the information relates. On August 14, 2024, this extensive review was completed. Since this time, Continuum has worked to verify the information and locate missing addresses in order to provide an accurate notice.

What Information Was Involved? Our review determined that the following types of information were present in the files that were accessed or acquired by the unauthorized actor: your name, health insurance information and medical information. Although the investigation was unable to confirm whether your information was actually viewed by the unauthorized actor, we are unable to rule out this possibility. Please note that Continuum is not aware of actual or attempted fraudulent misuse of any individual’s information as a result of this event.

What We Are Doing. The confidentiality, privacy, and security of personal information is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. Federal law enforcement is aware of this incident, and we also notified applicable regulators as required, including the U.S. Department of Health and Human Services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

000010102G0400

P

For More Information. If you have additional questions or need assistance, please call our dedicated assistance line at 1-833-961-7515 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding all major U.S. holidays. You may also write to Continuum at 404 Lippincott Drive, Marlton, New Jersey 08053.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Continuum Health

Steps You Can Take To Help Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

- 1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- 2. Social Security number;
- 3. Date of birth;
- 4. Addresses for the prior two to five years;
- 5. Proof of current address, such as a current utility bill or telephone bill;
- 6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
- 7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-h elp
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps their can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 11 Rhode Island residents that may be impacted by this event.