

HealthEC  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



31222

December 22, 2023

Dear [REDACTED]:

HealthEC, LLC (“HealthEC” or “We”) is a population health technology company that provides services to other entities, including [REDACTED]. We are writing to make you aware of a data incident that may impact the privacy of some of your information we received in connection to our relationship with [REDACTED].

**What Happened?** HealthEC became aware of suspicious activity potentially involving our network and promptly began an investigation. The investigation determined that certain systems were accessed by an unknown actor between July 14, 2023, and July 23, 2023, and during this time certain files were copied. We then undertook a thorough review of the files in order to identify what specific information was present in the files and to whom it relates. This review identified information relating to some of our clients. We began notifying our clients on October 26, 2023, and we worked with them to notify potentially impacted individuals, including you. The organization on whose behalf HealthEC is providing your notice is [REDACTED].

**What Information Was Involved?** Your name and [REDACTED] were present in the impacted files.

**What We Are Doing.** We take this event, your privacy, and the security of information in our care very seriously. Upon learning of the suspicious activity, we moved immediately to investigate and respond. The investigation included confirming the security of our network, reviewing the relevant files and systems, notifying potentially affected business partners/customers, and notifying federal law enforcement. As part of our ongoing commitment to your privacy and the security of information in our care, we are also reviewing our existing policies and procedures.

As an added precaution, we are offering twelve (12) months of credit monitoring and identity restoration services through TransUnion. If you wish to activate these complimentary services, you may follow the instructions included in the attached *Steps You Can Take to Protect Personal Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, health care provider, and/or financial institution. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

**For More Information.** If you have additional questions or concerns, please feel free to call us at 1-833-466-9216. We are available 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. You may also write to HealthEC at Attn: Cyber Notifications, 343 Thornall St., Suite 630, Edison, NJ 08837.

Sincerely,  
HealthEC



000010102G0400

P

## **STEPS YOU CAN TAKE TO PROTECT INFORMATION**

### **Enroll in Monitoring Services**

HealthEC is providing you with access to credit monitoring services through TransUnion 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. We are also providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through myTrueIdentity, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [www.mytrueidentity.com](http://www.mytrueidentity.com) and follow the instructions provided. When prompted please provide the following unique code to receive services: .

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](http://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.

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
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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 promptly 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; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 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](http://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>.

00001020280000

D

*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](http://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](http://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 451 Rhode Island residents that may be impacted by this event.

HealthEC  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



December 22, 2023

Dear [REDACTED]

HealthEC, LLC (“HealthEC” or “We”) is a population health technology company that provides services to other entities, including Beaumont ACO and Corewell Health. We are writing to make you aware of a data incident that may impact the privacy of some of your information we received in connection to our relationship with Beaumont ACO and Corewell Health.

**What Happened?** HealthEC became aware of suspicious activity potentially involving our network and promptly began an investigation. The investigation determined that certain systems were accessed by an unknown actor between July 14, 2023, and July 23, 2023, and during this time certain files were copied. We then undertook a thorough review of the files in order to identify what specific information was present in the files and to whom it relates. This review identified information relating to some of our clients. We began notifying our clients on October 26, 2023, and we worked with them to notify potentially impacted individuals, including you. The organization on whose behalf HealthEC is providing your notice is Beaumont ACO and Corewell Health.

**What Information Was Involved?** Your name and Name, Address, Date of Birth, Social Security Number, Medical Record Number, Medical information (such as Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider’s name), Health insurance information (such as beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and Claims information (such as patient account number, patient identification number, and treatment cost information) were present in the impacted files.

**What We Are Doing.** We take this event, your privacy, and the security of information in our care very seriously. Upon learning of the suspicious activity, we moved immediately to investigate and respond. The investigation included confirming the security of our network, reviewing the relevant files and systems, notifying potentially affected business partners/customers, and notifying federal law enforcement. As part of our ongoing commitment to your privacy and the security of information in our care, we are also reviewing our existing policies and procedures.

As an added precaution, we are offering twelve (12) months of credit monitoring and identity restoration services through TransUnion. If you wish to activate these complimentary services, you may follow the instructions included in the attached *Steps You Can Take to Protect Personal Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, health care provider, and/or financial institution. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

**For More Information.** If you have additional questions or concerns, please feel free to call us at 1-833-466-9216. We are available 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. You may also write to HealthEC at Attn: Cyber Notifications, 343 Thornall St., Suite 630, Edison, NJ 08837.

Sincerely,  
HealthEC

000010102G0400

P

## **STEPS YOU CAN TAKE TO PROTECT INFORMATION**

### **Enroll in Monitoring Services**

HealthEC is providing you with access to credit monitoring services through TransUnion 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. We are also providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through myTrueIdentity, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [www.mytrueidentity.com](http://www.mytrueidentity.com) 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.

### **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](http://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.

n 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
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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 promptly 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; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 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](http://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>.



00001020280000

P

*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](http://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](http://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 451 Rhode Island residents that may be impacted by this event.