Michele Veltri
Office: (267) 930-2297
Fax: (267) 930-4771
Email: mveltri@mullen.law

411 Theodore Fremd, Ste 206S
Rye, NY 10580

January 7, 2026

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Healthcare Interactive, Inc. ("HCIactive") located at 6011 University Boulevard, Suite 400, Ellicott City, Maryland 21043, and write to notify your office of an incident that may affect the security of certain personal information relating to ten thousand five hundred thirty-two (10,532) Iowa residents. HCIactive is providing notice on behalf of the following entities ("Clients") and the total number of impacted individuals, as noted in parenthesis below:

- HealthNow Administrative Services (163)

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, HCIactive does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 22, 2025, HCIactive became aware of suspicious activity related to its computer network. In response, HCIactive quickly worked to secure all systems and began an investigation to determine the full nature and scope of the activity. The investigation determined that between on or about July 8, 2025, and July 12, 2025, an unauthorized actor copied certain files from its computer network. Following this determination, HCIactive evaluated the impacted files and

determined that protected information was contained within the files that were potentially acquired by the unauthorized actor. While HCIactive is not aware of any actual or attempted misuse of information within its care, HCIactive provided notice to Clients and offered to provide notice to affected individuals on behalf of Clients. HCIactive is notifying you today on behalf of the Clients listed above.

While the protected information present within the potentially affected data varies by individual it can include name; date of birth; email address; phone number; mailing address; Social Security number; health insurance enrollment data (such as health plans/policies, insurance companies, and member/group ID numbers); medical data (such as medical record numbers, doctors, diagnoses, care, prescription information, and treatment); and health insurance claims data (such as claim numbers, account numbers, explanation of benefits, and billing codes). HCIactive coordinated notification with Clients and is providing notice to individuals and regulators, as directed, on behalf of Clients.

Notice to Iowa Residents

On or about December 2, 2025, HCIactive began providing written notice of this incident to Iowa residents. HCIactive continues to provide written notice of this incident and is expected to complete notice to approximately ten thousand five hundred thirty-two (10,532) Iowa residents in the coming days. 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, HCIactive moved quickly to investigate and respond to the incident, assess the security of HCIactive systems, and identify potentially affected individuals. Further, HCIactive notified federal law enforcement regarding the incident. HCIactive is also working to implement additional safeguards and training to its employees. HCIactive is providing access to credit monitoring services for twenty-four (24) months through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HCIactive is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HCIactive 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.

HCIactive is providing written notice of this incident to relevant state regulators, as necessary. HCIactive also posted about this incident on its website and notified prominent media throughout the United States. HCIactive also notified 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) 930-2297.

Very truly yours,

Michele Veltri

Michele Veltri of
MULLEN COUGHLIN LLC

MTV/mls
Enclosure

EXHIBIT A

Healthcare Interactive, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

December 5, 2025

NOTICE OF SECURITY INCIDENT

Dear

Healthcare Interactive, Inc. ("HCIactive") writes to inform you of an incident that may affect the security of your personal information. This letter provides details of the incident, our response, and resources available to you to help protect your personal information, should you feel it is appropriate to do so. HCIactive stores your personal information on its systems as it provides administrative services to

What Happened? On or about July 22, 2025, HCIactive became aware of suspicious activity related to its computer network. In response, we quickly worked to secure all systems and began an investigation to determine the full nature and scope of the activity. The investigation determined that between on or about July 8, 2025, and July 12, 2025, an unauthorized actor copied certain files from our computer network. Following this determination, we evaluated the impacted files and recently determined that your information was contained within the files that were potentially acquired by the unauthorized actor. While we are not aware of any actual or attempted misuse of information within our care, HCIactive is providing notice to you on behalf of

What Information Was Involved? The investigation determined the following types of your personal information were potentially impacted by the incident: your name in combination with

Again, there is no evidence that your personal information was subject to any actual or attempted misuse in connection with this incident.

What We Are Doing. We take this incident and the security of personal information in our care seriously. As part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to prevent similar future incidents. We are also reviewing and enhancing existing policies and procedures. As an added precaution, HCIactive is offering you complimentary access to months of credit monitoring through Cyberscout, a TransUnion company. Details of this offer and instructions on how to enroll are included below. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the offered identity monitoring services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your free credit reports, account statements and explanation of benefits forms for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to the applicable institute. Additional information and resources are included in the attached *Steps You Can Take to Help Protect Personal Information* portion of this notice.

P 0000101102G0500

For More Information. If you have questions, you may contact our dedicated assistance line at 1-833-855-4330, Monday through Friday from 8:00 a.m. ET to 8:00 p.m. ET (excluding major U.S. holidays). You may also write to HCIactive at 6011 University Boulevard, Suite 400, Ellicott City, Maryland 21043.

Sincerely,

Healthcare Interactive, Inc.

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 **https://bfs.cyberscout.com/activate** 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 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

0000102028000 P

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; 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 incident. There are approximately 0 Rhode Island residents that may be impacted by this incident.