EXHIBIT 1

We represent Inisightin Health, Inc. ("Insightin") located at 145 West Ostend Street, Suite 600 - #3425, Baltimore, Maryland 21230, and are writing to notify your office of an incident that may affect the security of certain personal information relating to eleven thousand seven hundred forty (11,740) Washington residents. Insightin is providing notice on behalf of its Covered Entity clients ("Clients").

Notice and 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, Insightin does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

In September 2025, Insightin identified suspicious activity within its networked environment after an unauthorized actor gained access to the Insightin network by exploiting a zero-day vulnerability in the GoAnywhere software. In response, Insightin launched an investigation with the assistance of third-party specialists into the nature and scope of this potential incident. Insightin determined that certain files stored on a limited number of Insightin servers may have been accessed or copied by an unauthorized party between September 17, 2025, and September 23, 2025. As a result, Insightin remediated to prevent the potential for ongoing access and began a comprehensive review of these files to determine whether sensitive information may be impacted, and whom that information belonged to. That investigation completed recently, and between December 4, 2025, and December 18, 2025, Insightin provided information about this incident to potentially impacted clients. Insightin then worked with its clients to compile and finalize lists of potentially impacted individuals to provide notification to impacted individuals.

Although the information varies for each individual, the potentially impacted data includes name, and date of birth, medical information and health insurance information. Insightin coordinated notification with Clients and is providing notice to individuals and regulators, as directed, on Client's behalf.

Notice to Washington Residents

As of March 4, 2026, Insightin has provided written notice regarding this incident to a total number of eleven thousand seven hundred forty (11,740) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification to individuals is ongoing and Insightin may supplement this notification if it is determined that a significant amount of March residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, Insightin moved quickly to investigate and respond to the incident, assess the security of Insightin systems, and identify potentially affected individuals and Insightin Clients. Further, Insightin notified federal law enforcement regarding the event and is also reviewing existing security policies and have implemented additional measures to further protect against similar incidents moving forwards, including additional safeguards and training to its employees. Insightin is providing access to credit monitoring services for twelve (12) months, through TrasnUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Insightin is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Insightin 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. Insightin is also notifying the U.S. Department of Health and Human Services, and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

Insightin Health, Inc
c/o Cyberscout

March 4, 2026

NOTICE OF DATA BREACH

Dear

Insightin Health, Inc. ("Insightin") is a vendor that provides data analytics and technology solutions designed to help healthcare payers improve member engagement, including your health plan. This letter is to inform you that a software Insightin used to exchange files with your health plan was recently involved in a cybersecurity incident that may have affected some of your personal information. Below you will find a brief summary of what happened, how we responded, and what you can do to protect yourself, if you wish.

What Happened? Insightin used a file-transfer tool called GoAnywhere to move data between Insightin and your health plan. On September 23, 2025, we identified unusual activity in our servers. Upon investigation, it was found that an unauthorized party gained access to GoAnywhere's file-transfer tool using an unknown design flaw in GoAnywhere's software. This allowed the party to potentially access data on a subset of our servers between September 17 and September 23, 2025. We immediately engaged third-party experts, stopped any further access, and began a thorough review of the affected files. On February 12, 2026, your health plan confirmed that some of your personal information was included in those files.

What Information Was Involved? Our investigation found that the affected files contained your personal information. This information may have included your name, health care provider name, insurance information and member ID. No Social Security numbers or financial information was involved.

What We Are Doing. Insightin is committed to protecting your information. After learning of the incident, we secured our environment, updated our security policies, and added new safeguards to prevent future incidents. We also reported the incident to law enforcement and regulators, as required. As a precaution, we are offering you twelve (12) months of free credit monitoring through Cyberscout, a TransUnion company. Instructions for enrollment are in the attached "Steps You Can Take to Help Protect Your Information". Please note that due to privacy restrictions, we are unable to automatically enroll you in the offered credit monitoring services.

What You Can Do. We invite you to enroll in the free credit monitoring services and to monitor your account statements and free credit reports for any unusual activity over the next 12-24 months. Please refer to the enclosed "Steps You Can Take to Help Protect Your Information" for additional guidance.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 844-784-5928, Monday through Friday, 8:00AM to 8:00PM, Eastern Time, except holidays. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you. You can also write to Insightin at 145 West Ostend Street, Suite 600 - #3425, Baltimore, Maryland 21230.

Sincerely,

Insightin Health

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation 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/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 1641 Rhode Island residents that may be impacted by this event.