Health Management Systems, Inc. (“HMS”)
225 E John W Carpenter Fwy Suite 500,
Irving, TX 75062

June 16, 2026

[Member Name]
[Member Address]

Important Notification – Please read this entire letter or Notice of Data Breach

Dear [Member],

On behalf of Health Management Systems, Inc. (“HMS”), I am writing to inform you about a recent incident that may have involved personal information about you.

HMS is contracted to provide Medicaid benefits administration services on behalf of health plans and may have processed your personal information if you have received Medicaid benefits.

We regret that this incident occurred and take the security of your personal information seriously.

WHAT HAPPENED. On April 21, 2026, we were informed that one of our employees uploaded a photo of their workstation to their Facebook account. Certain personal information about you, is visible in the photo the employee uploaded.

As soon as we became aware of the issue, we launched an investigation and took measures to restrict any further potential access to this data. We demanded and have received written confirmation that the employee removed the posting from Facebook, and that no copies of the photo were retained.

Through our investigation, we determined that the employee has “friend-only” access to their Facebook account, but your information could still have been visible to the employee’s friends. We are providing you with notice of this incident out of an abundance of caution.

WHAT INFORMATION WAS INVOLVED. We determined that the personal information associated with Facebook posting included your name, address, Social Security Number, claim number and that the billing provider was a behavioral health center. The disclosure did not state the type of medical services billed.

WHAT WE ARE DOING. We began investigating the incident as soon as we learned of it and took immediate corrective action to resolve the issue, including disciplinary action in accordance with our policies. We take the security of your personal information seriously and are committed

to safeguarding such information. We continue our efforts to enhance the protections in place to secure the information in our care.

WHAT YOU CAN DO. Consistent with certain laws, we are providing you with the following additional information about steps that individuals can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary identity theft protection service through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Activate this free service before August 15, 2026, using the following activation code: XXXXXXXX. This code is unique for your use and should not be shared. To enroll, visit https://app.idx.us/account-creation/protect or call toll-free to 1-800-939-4170. Representatives are available to provide assistance Monday through Friday between 8 a.m. and 8 p.m. Central Time, except major U.S. holidays.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www. ftc.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

A Gainwell Technologies Company

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.Equifax.com/personal/credit-report-services	www.Experian.com/help	Chester, PA 19022
		www.TransUnion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION.
Should you have any additional questions or concerns related to this matter, please contact me, or any other member of Gainwell's Compliance and Ethics Department, by phone 1-833-331-1349 or via email at compliance@gainwelltechnologies.com.

Again, we encourage you to take full advantage of this service offering.

We apologize for any inconvenience this may cause you.

Sincerely,

Marshall Preddy
Corporate Privacy Officer
Gainwell Technologies, Inc.
(Enclosure)