Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

June 15, 2023

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 Harvard Pilgrim Health Care ("Harvard Pilgrim") located at 1 Wellness Way, Canton, MA 02021, and are writing office on behalf of Harvard Pilgrim and its applicable business associates to notify your office of an incident that may affect the security of certain personal information and/or protected health information relating to one thousand three hundred nineteen (1,319) Iowa 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, Harvard Pilgrim 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 April 17, 2023, Harvard Pilgrim discovered it was the victim of a cybersecurity ransomware incident that impacted systems used to service members, accounts, brokers and providers. After detecting the unauthorized party, Harvard Pilgrim proactively took its systems offline to contain the threat. Harvard Pilgrim notified law enforcement and regulators and is working with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation.

Harvard Pilgrim is continuing its active investigation and conducting extensive system reviews and analysis before it can resume its normal business operations. Unfortunately, the investigation identified signs that data was copied and taken from Harvard Pilgrim systems from March 28, 2023 to April 17, 2023. Harvard Pilgrim determined that the files at issue may contain personal information and/or protected health information. The investigation revealed that the following information related to Harvard Pilgrim members could potentially be in the files at issue: member names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names).

Notice to Iowa Residents

On May 23, 2023, Harvard Pilgrim began notifying potentially impacted individuals by posting notice to its website, providing notice to statewide media in all fifty (50) states and notifying providers, brokers and employer groups. Included in the employer group notice was a message to be sent directly to employees as Harvard Pilgrim did not have direct access to member email addresses. On or about June 15, 2023, Harvard Pilgrim began providing written notice of this incident to one thousand three hundred nineteen (1,319) Iowa residents for whom it believes it has valid mailing addresses. 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, Harvard Pilgrim moved quickly to investigate and respond to the incident, assess the security of Harvard Pilgrim systems, and identify potentially affected individuals. Further, Harvard Pilgrim notified federal law enforcement regarding the event. Harvard Pilgrim is also working to implement additional safeguards and training to its employees. Harvard Pilgrim is providing access to credit monitoring services for two (2) years, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

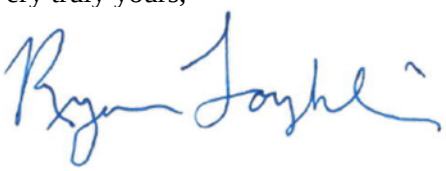
Additionally, Harvard Pilgrim is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Harvard Pilgrim is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national 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.

Harvard Pilgrim 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. Harvard Pilgrim also notified the U.S. Department of Health and Human Services and prominent media 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) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/kzf
Enclosure

EXHIBIT A

Harvard Pilgrim Health Care

Return to IDX
PO Box 480149
Niles, IL 60714

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

To Enroll, Please Call:
(888) 220-5517
Or Visit:
https://response.idx.us/HPHC
Enrollment Code: [XXXXXXXX]

June 15, 2023

Dear <First Name> <Last Name>,

We are writing to inform you of a cybersecurity incident experienced by Harvard Pilgrim Health Care ("Harvard Pilgrim") that may involve your personal information and/or protected health information. We are providing information about the measures we have taken in response to the incident, and steps you can take to help protect yourself against possible misuse of information.

What Happened

On April 17, 2023, Harvard Pilgrim discovered it was the victim of a cybersecurity ransomware incident that impacted systems used to service members, accounts, brokers and providers. After detecting the unauthorized party, we proactively took our systems offline to contain the threat. We notified law enforcement and regulators and are working with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation.

We take the privacy and security of the data entrusted to us seriously. We are continuing our active investigation and conducting extensive system reviews and analysis before we can resume our normal business operations. Unfortunately, the investigation identified signs that data was copied and taken from our Harvard Pilgrim systems from March 28, 2023, to April 17, 2023. We determined that the files at issue may contain your personal information and/or protected health information.

What Information Was Involved

The personal information and/or protected health information in the files at issue may include your name, physical address, phone number, date of birth, health insurance account information, Social Security number, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names). We are not aware of any misuse of your personal information or protected health information as a result of this incident.

What We Are Doing

As explained above, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we implemented and/or are continuing to implement additional cybersecurity safeguards to our existing robust infrastructure to better minimize the likelihood of this type of event occurring again.

What You Can Do

We recommend that you remain vigilant, monitor and review all of your financial and account statements and explanations of benefits, and report any unusual activity to the institution that issued the record and to law enforcement. You may also review the guidance contained in *Steps You Can Take to Protect Personal Information.*

Additionally, we are providing you with the opportunity to register for two (2) years of complimentary credit monitoring and identity protection services through IDX. Although we are making these services available to you, we are unable to enroll you directly. For enrollment instructions, please review the information contained in the attached *Steps You Can Take to Protect Personal Information*. If you are already enrolled in the complimentary credit monitoring and identity protection services provided, you do not need to enroll again.

For More Information

The security of your protected health information is a top priority for us. We sincerely regret this incident occurred and for any concern it may cause you. We understand that you may have additional questions. For assistance with questions regarding this incident, please call IDX at (888) 220-5517 or go to https://response.idx.us/HPHC. Representatives are available between the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday (excluding U.S. holidays).

Sincerely,

Christopher Walsh
VP, Privacy & Fraud Prevention and Recovery
Point32Health

Steps You Can Take To Protect Personal Information

Services Being Offered By Harvard Pilgrim

Enrollment Code: [Code Here]

Go to https://response.idx.us/HPHC and follow the instructions for enrollment using your Enrollment Code above. Additionally, you may call the IDX call center at (888) 220-5517 (toll free), Monday through Friday from 9:00 a.m. to 9:00 p.m. ET, excluding U.S. holidays. If you are already enrolled in the complimentary credit monitoring and identity protection services provided, you do not need to enroll again. Please note the deadline to enroll is November 23, 2023.

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. A security freeze essentially blocks any potential creditors from being able to view or pull your credit file unless you affirmatively unfreeze or thaw your file beforehand. Having a freeze in place does nothing to prevent you from using existing lines of credit you may already have, such as credit, mortgage and bank accounts. When you place a freeze, each credit bureau will assign you a personal identification number (PIN) that needs to be supplied when you open a new line of credit. When that time comes, consumers can temporarily thaw a freeze for a specified duration either online or by phone. 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. The following is information required by applicable state law:

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.

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, 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.