150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

August 11, 2023

Michael Waters
312-463-6212
312-819-1910 Direct Fax
mwaters@polsinelli.com

VIA E-MAIL (CONSUMER@AG.IOWA.GOV)
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319

Re: ***Notification of a Potential Data Security Incident***

Dear Madam/Sir:

We represent BrightSpring Health Services ("BrightSpring"), which has a mailing address of 805 N. Whittington Parkway Louisville, KY 40222, in connection with a recent data incident that impacted BrightSpring and its subsidiary, PharMerica. BrightSpring is reporting this incident pursuant to Iowa Code § 715C.1-2. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While BrightSpring is notifying you of this incident, BrightSpring does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE INCIDENT

On March 14, 2023, BrightSpring learned of suspicious activity on a computer network that it shares with its subsidiary, PharMerica. Upon discovering the incident, BrightSpring promptly began an internal investigation and engaged cybersecurity experts to investigate and secure its computer systems. The investigation determined that an unknown third party accessed BrightSpring's computer systems from March 12-13, 2023, and that certain data may have been obtained as a part of the incident. On May 20, 2023, BrightSpring identified a population whose personal information was contained in the involved data. On June 12, 2023, as its review of the involved data continued, BrightSpring identified additional individuals whose personal information was contained in the involved data. The involved personal information varied by person but for each person included name, address, date of birth, and/or Social Security number.

At this point, BrightSpring is not aware of any fraud or identity theft to any individual as a result of this incident, but nonetheless has begun notifying potentially affected individuals to provide

them with more information and resources. BrightSpring has also arranged for complimentary identity protection and credit monitoring services for potentially affected individuals. The notice includes information on steps individuals can take to protect themselves against potential fraud or identity theft.

NOTICE TO IOWA RESIDENTS

BrightSpring is notifying one thousand five hundred seventy-two (1,572) residents' whose personal information was contained in the data potentially acquired by an unauthorized party. BrightSpring is providing these notifications via letters sent by first-class United States mail. BrightSpring started mailing these letters on June 21, 2023 and expects to complete the mailing today, August 11, 2023. The notification letters include information on how to protect against fraudulent activity and identity theft, as well as an offer for complimentary credit monitoring and identity theft protection services. The notification letters also include a phone number for individuals to call with any questions they may have regarding the incident. Enclosed is a sample of the notification letter.

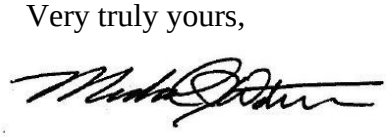
STEPS TAKEN RELATING TO THE INCIDENT

Upon discovering the incident, BrightSpring promptly began an internal investigation and engaged cybersecurity experts to investigate and secure its computer systems. As explained above, BrightSpring is notifying individuals whose personal information was contained in the data potentially acquired by an unauthorized party, providing them with information about how to protect against fraudulent activity and identity theft, and is offering them complimentary credit monitoring and identity theft protection services. BrightSpring has also notified law enforcement and is evaluating additional controls it can implement to reduce the risk of a similar incident occurring in the future.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,



Michael J. Waters

Enclosure

BRIGHTSPRING HEALTH SERVICES

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

BrightSpring Health Services values and respects the privacy of your information, which is why we are writing to advise you of an incident that may have involved some of your personal information. **While we have no reason to believe that your information has been misused for the purpose of committing fraud or identity theft,** we are writing in accordance with relevant law to advise you about the incident and to provide you with guidance on what you can do to help protect yourself, should you feel it is appropriate to do so.

What Happened? On March 14, 2023, we learned of suspicious activity on our computer network. Upon discovering the cybersecurity incident, we promptly began an internal investigation and engaged cybersecurity advisors to investigate and secure our computer systems. The investigation determined that an unknown third party accessed our computer systems from March 12 to 13, 2023, and that certain personal information may have been obtained from our systems as a part of the incident. Following further investigation, we recently discovered that certain files that included employee information were involved in the incident, which is why we are writing to you now.

What Information Was Involved? We have been conducting a comprehensive review of the potentially affected data to determine whose personal information may have been obtained. On June 12, 2023, we determined that the data included files that included your name and Social Security number. For some individuals, the files also contained an address and/or date of birth. The files did not contain financial information or health information.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident from occurring in the future, including enhancing our technical security measures. We are also offering a complimentary one-year membership of identity monitoring through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to take advantage of the complimentary identity monitoring included in this letter. You can also find more information on steps to help protect yourself against possible identity theft or fraud in the *Additional Important Information* section below.

For More Information. We value the trust you place in us to help protect your privacy, take our responsibility to safeguard your personal information seriously, and deeply regret any inconvenience this incident might cause. For further information and assistance, please call (866) 547-6904 from 8 a.m. to 5:30 p.m. CST, Monday through Friday, excluding major U.S. holidays.

Sincerely,

BrightSpring Health Services

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. As the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

This notice was not delayed at the request of law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected XX Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. 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.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.