Preferred Care
HOME HEALTH SERVICES

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

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

Re: Notification of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a recent data security incident experienced by Preferred Care Home Health Services ("Preferred Care") that may have involved your personal or health information. At Preferred Care, we are committed to the security of all information within our possession. This is why we are writing to notify you of this incident and to inform you about steps that can be taken to help safeguard your information.

What Happened? On April 30, 2020, we detected unusual email account activity. Upon discovering this activity, we immediately took steps to secure our email system and launched an investigation. We hired a leading, independent computer forensics firm to determine what happened and whether sensitive information was accessed without authorization. As a result of this investigation, we learned that a limited number of Preferred Care employee email accounts were accessed without authorization between approximately January 13, 2020 and April 27, 2020. We then engaged a data review firm to review the contents of the accounts and discovered on August 4, 2020 that the accounts contained some of your personal or health information which may have been accessed without authorization. We then worked diligently through August 28, 2020, to identify current mailing address information so that we could notify potentially affected individuals.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems. In addition, we are not aware of the misuse of any potentially impacted information.

What Information Was Involved? The information may have involved your <<b2b_text_1(ImpactedData)>>.

What We Are Doing. As soon as we discovered this incident, we took the measures described above and implemented enhanced security measures to help prevent a similar incident from occurring in the future. We also reported this matter to the Federal Bureau of Investigation and will fully cooperate with any investigation. In addition, we are providing information about steps that you can take to help protect your personal information.

What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your personal information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please call Kroll at 1-???-???-????, Monday through Friday from 8:00 am to 5:30 pm Central Time. Kroll representatives are fully versed on this incident and can answer questions or concerns you may have regarding the protection of your personal information.

Thank you for your patience through this incident. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this incident may cause you.

Sincerely,

Jay Larson
Privacy Officer
Preferred Care Home Health Services

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 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 this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

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

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.