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

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

Notice of Data Breach

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

We are writing to notify you of an incident that may affect the privacy of some of your information. While, to date, we have no evidence that information potentially affected by this incident has been misused, we take this incident very seriously and are providing you with details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What happened?

On February 24, 2022, Covenant Care California, LLC ("Covenant") learned that an employee of Wagner Heights Nursing and Rehabilitation Center had experienced suspicious activity within her email account. Immediate steps were taken to secure the account and we promptly commenced an investigation to determine the nature and scope of the incident. Working with our Information Technology ("IT") Director, IT support services, and third-party forensic investigators, we determined that an unauthorized actor(s) gained access to the employee's email account for several hours via a phishing email on February 24, 2022. We then undertook a diligent review and analysis of the email account to determine the full nature and scope of the security incident, including what records were present in the account at the time of unauthorized access, to whom those records relate, and what information the records contained. Through this review, on April 18, 2022, we determined that certain patient records were present in the account at the time of the unauthorized access. Based on our investigation, Covenant confirmed that your information was present in the account. While, to date, we are unaware of any actual or attempted misuse of information potentially affected by this incident, we are providing you this notification out of an abundance of caution.

What information was involved?

Below is a list of your information present in the account at the time of the unauthorized access:

<<b2b_text_1 (Data Elements)>><<b2b_text_2 (Data Elements cont.)>><<b2b_text_3 (Data Elements cont.)>>

What we are doing.

Information privacy and security are among our highest priorities. Wagner Heights Nursing and Rehabilitation Center's technical, administrative, and physical safeguards are being reviewed to identify and implement any potential enhancements to its security measures, including installation of additional technical safeguards to our email systems. Further, our general privacy and security policies and procedures are being reviewed for potential enhancements, as well as our policies and procedure specific to employee training on email security. Finally, additional employee retraining is being conducted regarding email safety and security awareness.

As indicated above, upon learning of this incident, we quickly took steps to secure the affected email account and initiated a thorough investigation. Our investigation is ongoing and we are working with forensic investigators and other third-party vendors to assist with the investigation, mitigation, and remediation activities. We are also reporting this incident to law enforcement and appropriate state and federal regulators.

We are providing you with notice of this incident and with information and resources you may use to better protect against potential misuse of your information, should you feel it appropriate to do so. As an added precaution and to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Identity Monitoring at no cost to you for one year. Kroll provides security incident mitigation and response services and their team has extensive experience helping people who have sustained an unintentional exposure of information. 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 (Date)>>** *to activate your Identity Monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, please visit info.krollmonitoring.com. In addition, please review the attached "Additional Resources" regarding steps you can take to protect your information".

What you can do.

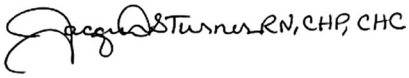
We encourage you to activate the Kroll Identity Monitoring services that we are offering as we are not able to act on your behalf to do so. Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line (855) 788-2390, (toll free), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,



Jacqueline Turner, R.N.
Covenant Care Privacy Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. **This notice has not been delayed by law enforcement**.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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.