NORTHGAUGE
HEALTHCARE ADVISORS
A COKER COMPANY

February 25, 2025

Office of the Attorney General
Washington State
1125 Washington St. SE
PO Box 40100
Olympia, WA
98504

To whom it may concern:

The purpose of this letter is to provide notice to the Washington State Office of the Attorney General, in accordance with R.C.W. § 19.255.010, of a data breach impacting CommonSpirit Health. This data breach is being reported on CommonSpirit Health's behalf by Northgauge Healthcare Advisors ("Northgauge"), a vendor of CommonSpirit Health. Northgauge is providing notice via the online reporting form available at https://fortress.wa.gov/atg/formhandler/ago/databreachnotificationform.aspx.

On November 25, 2024, Pinnacle Holdings, LTD ("Pinnacle"), a healthcare consulting company and vendor of Northgauge, experienced a network disruption that impacted certain systems on its network. Pinnacle immediately isolated its network and implemented additional security measures to protect its network against future security incidents. Pinnacle also engaged a third-party vendor to review the incident, and the vendor determined that a threat actor accessed a portion of Pinnacle's network and copied certain information containing personal information. Pinnacle provided notice of this incident to affected customers, including NorthGauge. NorthGauge had engaged Pinnacle to perform certain consulting services in connection with its work performed for CommonSpirit Health. NorthGauge has in place strict policies and procedures governing data retention and destruction.

Although Pinnacle initially provided notice to Northgauge in November 2025, confirmation and identification of impacted individuals were delayed until January 30, 2026. CommonSpirit Health was notified by Northgauge on February 2, 2026 of the Washington residents impacted by the incident.

Notification to Washington residents will be made as soon as contact information for affected individuals has been confirmed. Individuals will be offered credit monitoring services and will also be notified of the contact information for the major credit reporting agencies.

Please feel free to contact DeAnn Tucker with any questions at 2400 Lakeview Parkway, Suite 400 Alpharetta, GA 30009 and telephone number (800) 345-5829.

PINNACLE

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

9085 EAST MINERAL CIRCLE, SUITE 110
CENTENNIAL, CO 80112
www.AskPHC.com

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

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

Dear <<First_name>> <<Last_name>>:

Pinnacle Holdings, LTD provides healthcare consulting services to <<b2b_text_1 (Entity Name)>> and writes to notify you of an incident that may impact the privacy of certain information provided to us. We are providing you information about the incident, our response, and steps you can take to protect your information.

On November 25, 2024, we experienced a network disruption that impacted certain systems. Upon discovery, we took immediate action to address and investigate the event, which included engaging third-party specialists to assist with determining the nature and scope of the incident. The investigation determined that limited information maintained on our network may have been copied by an unauthorized actor between November 11, 2024, and November 25, 2024. Therefore, we reviewed the information potentially involved to determine the type(s) of data contained within and to whom that information pertained. The information may have included your name and the following: <<b2b_text_2 (Data Elements)><<b2b_text_3 (Data Elements cont.)>>.

We have taken steps to address the incident and are committed to protecting the information entrusted to us. Upon learning of this incident, we immediately began an investigation and reported this incident to law enforcement. We have also implemented additional safeguards to further enhance the security of information in our possession and to help prevent similar incidents from occurring in the future. Additionally, we are offering you free credit monitoring and identity protection services for <<ServiceTerminMonths>> months. Information about these services and instructions regarding how to enroll are included in the enclosed *Steps You Can Take to Help Protect Your Information*.

In addition to enrolling in the free credit monitoring and identity protection services, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity, please promptly contact the financial institution or company. We have also provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

We take the security of information entrusted to our care very seriously. While it is regrettable that this incident occurred, please be assured we are taking appropriate actions to rectify the situation and help prevent future incidents. If you have any questions or concerns, please contact our dedicated call center at (866) 686-2607 between the hours of 7:00 AM and 4:30 PM Mountain Time, Monday through Friday, excluding major U.S. holidays, or write us at 9085 E. Mineral Circle, Suite 110, Centennial, CO 80112.

Sincerely,

Pinnacle Holdings, LTD.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Instructions

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. 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.

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.

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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com	**Experian** 1-888-397-3742 www.experian.com	**Equifax** 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. <<b2b_text_4 (There are [#] Rhode Island residents impacted by this incident.)>>

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection.