Appendix

Covenant Health was first alerted to unusual activity in its Information Technology ("IT") environment on May 26, 2025, and immediately worked to secure and restore its systems. Industry-leading third-party information technology and forensic specialists were engaged to conduct a thorough investigation into the source and extent of the incident, including the amount and type of data that may have been affected. On December 10, 2025, through its ongoing extensive data analysis, Covenant Health and its third-party forensic specialists determined that patient information, including that of 41 Nebraska residents,[1] may have been involved in the incident.

Covenant Health further determined that an unauthorized party gained access to its IT environment on May 18, 2025, and was able to access some patient information. Covenant Health analyzed the data involved and completed the bulk of its data analysis. The involved data included patients' names and one or more of the following: addresses, dates of birth, medical record numbers, Social Security numbers, health insurance information, and treatment information, such as diagnoses, dates of treatment, and/or type of treatment.

On July 11, 2025, Covenant Health began notifying individuals affected by this incident while continuing to analyze the data involved. On December 31, 2025, Covenant Health mailed letters to individuals whose information was involved, including the 41 Nebraska residents, in accordance with the Health Insurance Portability and Accountability Act (45 CFR § 164.404) and Neb. Rev. Stat. § 87-803. A sample copy of the notification letter is enclosed. Covenant Health is offering complimentary credit monitoring and identity protection services to the Nebraska residents whose Social Security numbers may have been involved. Covenant Health has also established a dedicated, toll-free call center to address questions about the incident.

Covenant Health has enhanced the security of its IT environment to help prevent something like this from happening again.

---

[1] This report does not waive Covenant's objection that Nebraska lacks personal jurisdiction over it related to any claims that may arise from this incident.

COVENANT HEALTH
Our Name is Our Promise

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Covenant Health, Inc. (“Covenant Health”) and its affiliated entity, <<Variable Data 1>>, are committed to protecting our patients’ information. We are writing to inform you of a data security incident involving some of your information. This letter explains the incident, measures we have taken, and some steps you can take in response.

What Happened? On December 10, 2025, through its ongoing extensive data analysis, Covenant Health and its third-party forensic specialists determined your information may have been involved in a data security incident that occurred earlier this year. Covenant Health was alerted to unusual activity in our Information Technology (“IT”) environment on May 26, 2025, and immediately worked to secure and restore our systems. We engaged industry-leading third-party information technology and forensic specialists to conduct a thorough investigation into the source and extent of the incident, including the amount and type of data that may have been affected. Through that investigation, we learned that an unauthorized party gained access to our IT environment on May 18, 2025, and was able to access some patient information.

What Information Was Involved? The investigation determined that your information may have been obtained by the unauthorized party and may have included your name, address, date of birth, medical record number, Social Security number, health insurance information, and/or treatment information, such as diagnoses, dates of treatment, and type of treatment.

What We Are Doing: Covenant Health takes this event and the security of your information seriously. Upon learning of this event, we moved quickly to investigate and respond to the incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. We additionally engaged leading third-party forensic security experts to analyze the substantial amount of data impacted. That review is ongoing. Finally, we have enhanced the security of our IT environment to help prevent something like this from happening again.

Notice was also provided to federal law enforcement and appropriate agencies, and we remain committed to fully complying with all state and federal requirements.

What You Can Do: Although we are unaware of any fraudulent misuse of personal information relating to this event, out of an abundance of caution, we are offering you a complimentary one-year membership to Experian®’s IdentityWorks℠. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is free and enrolling in this program will not affect your credit score.

For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership and steps you can take in response, please see the pages that follow this letter.

Please also review the enclosed *Additional Steps You Can Take*, which contains information on what you can do to better protect against possible misuse of your information. We also recommend that you review the statements you receive from your health insurer. If you see services you did not receive, please contact your insurer immediately.

For More Information: We understand that you may have questions about this incident that are not addressed in this letter. We have established a dedicated call center and encourage you to call 1-855-361-0344, Monday through Friday, between 9:00 a.m. – 9:00 p.m., Eastern Time, should you have additional concerns.

We are committed to the safety of our patients and their personal information and sincerely regret any concern this incident may have caused you.

Sincerely,

Janice Bosteels

Janice Bosteels
System Chief Compliance & Privacy Officer

CREDIT MONITORING INFORMATION

We are offering a **complimentary** one-year membership to Experian IdentityWorks℠. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks In Three Easy Steps

1. ENROLL by: **<<Enrollment Deadline>> (**Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **<<Activation Code>>**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com/get-credit-report, 1-833-799-5355

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general 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 one-year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one-year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. *How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com/credit-freeze

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. *How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Covenant's mailing address is 40 Shattuck Road, Ste. 317 Andover, MA 01810 and its phone number is 978-312-4300.

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.