<<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>> <<last_name>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain what happened, what steps we are taking in response to the security incident, and how you can help protect yourself.

What happened?

On April 3, 2025, Cumberland County Hospital (CCH) discovered unauthorized access by a third party to our computer system. We immediately shut down all computers, disabled data sharing connections, contacted law enforcement, and began investigating. Our IT team worked around the clock with outside cybersecurity experts to restore secure access, to determine what happened, and to implement enhanced measures to prevent a similar incident from happening again. Cybersecurity experts determined that the unauthorized access to our computer system began on February 21, 2025 and ended on April 3, 2025.

What information was involved?

The electronic medical records system that CCH and its partners use to record and bill for patient care was not involved or accessed in this incident. However, there was unauthorized access to other files on our computer system that contain personally identifiable information, including health information. The information involved varies by individual but may have included demographic information (such as name, date of birth, address, phone number, email address, race or ethnicity), Social Security number, clinical information (such as medications, diagnoses, treatment notes, and dates of service), medical record number, health plan number, claims and billing information.

What we are doing.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services, including Credit Monitoring, Fraud Consultation, and Identity Theft Restoration, at no cost to you for 24 months. We encourage you to take full advantage of this service by contacting Kroll with any questions and activating the free identity monitoring services. Kroll representatives have been fully briefed on the incident and can answer questions or concerns you may have regarding the security of your personal information.

- 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>>**

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. 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.

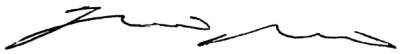
Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call (866) 461-3127, 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 take the confidentiality and security of our patients' information very seriously and regret any inconvenience this incident may have caused. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,



Richard Neikirk, CEO

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. By law, you are entitled to 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, visit **www.AnnualCreditReport.com** or call toll free at **1-877-322-8228**. Currently, all three credit reporting bureaus provide a weekly free credit report online. 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.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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 can 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. 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 FTC webpage provide consumers with information on how to prevent or minimize the risks of identity theft.

For Kentucky residents: You may report identity theft to the Attorney General of Kentucky by completing an online complaint form at https://secure.kentucky.gov/formservices/AttorneyGeneral/ScamReport or by calling the toll-free Identity Theft Hotline at 1-800-804-7556. Tips and additional resources for protecting yourself from or responding to identity theft are available at https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx.

For Tennessee residents: You may contact the Tennessee Identity Crimes Unit at 1150 Foster Ave., Cooper Hall, Nashville, TN 37243, Safety.IdentityCrime@tn.gov or visit the TN Department of Safety & Homeland Security webpage for additional Identity Theft Resources at https://www.tn.gov/safety/tnhp/sib/icu.html.

For Indiana residents: You can file an identity theft complaint with the Indiana Attorney General's Office online at https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/complaint-form/. You can also request a complaint form by calling (800) 382-5516 or (317) 232-6330.

For Ohio residents: You may request assistance from the Identity Theft Unit of the Ohio Attorney General's Consumer Protection Section by filing an Identity Theft Notification and Affidavit together with a submitting a police report. To download the Affidavit, go to https://www.ohioattorneygeneral.gov/identitytheft.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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 will 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.