WILMERHALE

June 22, 2026

Via Email

Kirk J. Nahra

+1 202 663 6128 (t)
+1 202 663 6363 (f)
kirk.nahra@wilmerhale.com

Office of the Attorney General
ATTN: Attorney General John M. Formella
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Breach Notification Update

To Whom It May Concern:

I am writing on behalf of my client Cerner Corporation ("Cerner") in follow-up to a notice that Cerner submitted to your office on December 19, 2025 via letter regarding a security incident that may have involved the protected health information ("PHI") of residents in your state.

Cerner provides software and services to health care providers and, in that role, acts as a business associate under the Health Insurance Portability and Accountability Act ("HIPAA") when delivering services to its covered entity customers. Cerner has offered to assume individual and regulatory notice obligations on behalf of the covered entity customers it notified as having been potentially impacted by the security event. Over the past several months, Cerner has continued conducting extensive data review and analysis and closely coordinating with its covered entity customers. These activities have included identifying potentially impacted individuals, obtaining their contact information, and supporting the mailing process for customers that delegated their individual notification obligation to Cerner so that letters could be mailed on a rolling basis. At this point in time, Cerner believes that the mailings on behalf of customers with potentially impacted patients in your state are substantially complete and is providing an update to the approximate number of individual notice letters that have been mailed to addresses in New Hampshire.

Cerner has provided notice to 60,247 individuals in your state, as measured by the number of letters Cerner has mailed[1] on behalf of covered entity customers that delegated individual notice obligations to Cerner. To the extent there is a material change to the information provided in this letter, Cerner will follow up accordingly.

* * *

[1] This number does not include letters that were later determined to have been mailed to an incorrect address by a customer, and where Cerner later facilitated a new round of mailings to individuals at the correct addresses. Only that second mailing for this particular customer is included in the count provided here.

Cerner does not intend to, and does not, waive any applicable privilege. If it were found that any of the information provided constitutes disclosure of otherwise privileged matters such disclosure would be inadvertent.

Please do not hesitate to contact me if you have any questions.

Best Regards,

Kirk J. Nahra

Kirk J. Nahra

[redacted]

July 25, 2025

Reference Number: [Internal ID]

N6669-L01-0000001 P001 T00001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - [redacted]
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Notice of Data Breach

Dear Sample A. Sample:

[redacted] is committed to safeguarding the privacy and confidentiality of your patient information. We were recently informed of a data security breach experienced by our electronic health record (EHR) vendor, Cerner, that may have included some of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against potential identity theft and fraud, should you feel it is appropriate to do so.

WHAT HAPPENED. On March 7, 2025, we learned that an unauthorized third party gained access to and obtained data that was maintained by our vendor. The vendor's investigation determined that the unauthorized third party gained access to personal health information on legacy Cerner systems at least as early as January 22, 2025. [redacted] computer systems were not impacted in this incident. The vendor later informed us that federal law enforcement asked to delay patient notification as they continued their investigation. As a result, we are notifying you now.

WHAT INFORMATION WAS INVOLVED. The personal information involved in this incident may have included your name, Social Security number, and information included within patient medical records, such as medical record numbers, doctors, diagnoses, medicines, test results, images, care and treatment.

WHAT WE ARE DOING. We began investigating the incident as soon as we learned of it. In addition, the vendor initiated its critical incident response process, took steps to secure the impacted systems, began an investigation, and worked with external cybersecurity specialists and federal law enforcement.

WHAT YOU CAN DO. To help protect your identity, you are being offered complimentary access to Experian IdentityWorks℠ Credit Plus 3B for 24 months in eligible jurisdictions. Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [redacted]. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. See Appendix for additional details.

FOR MORE INFORMATION. If you have further questions or concerns, or would like an alternative to enrolling online, please call [redacted] toll-free Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays). Please be prepared to provide your engagement number ENGAGE#.

We sincerely apologize for this incident and assure you that protecting your information remains a top priority for [redacted]

Sincerely,

[redacted]

0000001

ENGAGE#

N6669-L01

Activate IdentityWorks Credit Plus 3B Now in Three Easy Steps

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** January 31, 2026 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bplus
- Provide your **activation code**: ABCDEFGHI

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 [redacted] by January 31, 2026 (5:59 UTC). Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITY WORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. In addition to taking steps to protect your identity, be sure that bills and accounts look correct. We include steps on how to do that in this letter. If you learn of a crime against you, you can file a report with law enforcement.

*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.

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Order Your Free Credit Report

You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 888-4213
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
www.Equifax.com	www.Experian.com	www.TransUnion.com

You also have other rights under the Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your- rights-under-fcra.pdf.

Contact the U.S. Federal Trade Commission

You may contact the Federal Trade Commission ("FTC"), law enforcement, or your state Attorney General to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Fraud Alerts and Security Freezes

You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information at no cost to you. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

You can also contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report free of charge. You must separately place a credit freeze on your credit file at each credit reporting agency. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. After receiving your request, the credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place. If you request a lift of the credit freeze online or by phone, the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, the credit reporting agency must place or lift the credit freeze no later than three (3) business days after getting your request.

State Specific Information

For residents of the *District of Columbia, Iowa, Maryland, New York, North Carolina, Oregon and Rhode Island*

You may contact your Attorney General for additional information about avoiding identity theft. If you are a Rhode Island resident, you may also file a police report by contacting local or state law enforcement agencies.

You may use the following information to contact your attorney general:

District of Columbia	**Iowa**	**Maryland**	**Oregon**
Office of the Attorney General Office of Consumer Protection 400 6th Street, NW Washington, DC 20001 (202) 442-9828 www.oag.dc.gov	Office of the Iowa Attorney General Hoover State Office Building 1305 E. Walnut Street Des Moines, IA 50319 (515) 281-5926 / (888) 777-4590 www.iowaattorneygeneral.gov	Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (410) 528-8662 www.marylandattorneygeneral.gov	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (877) 877-9392 www.doj.state.or.us
New York	**New York**	**North Carolina**	**Rhode Island**
New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway, 3rd Floor New York, NY 10271 (800) 771-7755 www.ag.ny.gov	New York Department of State Division of Consumer Protection 99 Washington Avenue Suite 650 Albany, New York 12231 (800) 697-1220 www.dos.ny.gov	North Carolina Department of Justice 9001 Mail Service Center Raleigh, NC 27699-9001 (919) 716-6000 www.ncdoj.gov	Rhode Island Office of the Attorney General Consumer Protection Division 150 South Main Street Providence, RI 02903 (401) 274-4400 www.riag.ri.gov

For residents of *Massachusetts*: Under Massachusetts law, you have the right to obtain any police report filed in connection with the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.