

Appendix

The Board of Regents of the University of Nebraska for and on behalf of the University of Nebraska Medical Center (“UNMC”) maintains computer software applications that support research studies, quality improvement projects, and public health activities, including REDCap. UNMC is a covered entity under the Health Insurance Portability & Accountability Act (“HIPAA”).

In February 2026, UNMC learned that REDCap had a vulnerability that could allow an unauthorized person to gain remote access to the application. As soon as UNMC learned of this issue, it took REDCap offline and began an investigation with privacy and cybersecurity partners. On February 18, 2026, the investigation determined that REDCap was subject to unauthorized access between September 20, 2023 and February 3, 2026. The investigation was unable to conclusively determine whether specific records stored in REDCap were viewed or taken.

The information that may have been involved varied by project and individual. It may have included the name; Social Security number; identifiers such as date of birth, address, phone number, email address, and/or medical record number; and information created or collected in connection with a research study, such as clinical information, visit dates, diagnoses, medications, laboratory results, imaging or procedure information, questionnaire responses, or other health-related information of 186 Nebraska residents.¹

On April 17, 2026 UNMC began mailing notification letters to affected individuals via the United States Postal Service First-Class mail in accordance with HIPAA (45 CFR § 164.404) and/or Neb. Rev. Stat. § 87-803. A copy of the notification letter is enclosed. UNMC is offering individuals whose Social Security number was contained in REDCap with access to complimentary credit monitoring and identity theft prevention services. Additionally, UNMC has established a dedicated, toll-free call center to answer questions that individuals may have about the incident.

To help prevent a similar incident from occurring in the future, UNMC moved REDCap to an updated version of REDCap that was released to address the vulnerability. The new version of REDCap has enhanced logging and security controls enabled.

¹ Please note, additional Nebraska residents are receiving notice of this incident pursuant to HIPAA, but the information involved for these individuals does not constitute “personal information” as defined by Neb. Rev. Stat. § 87-802(5).



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

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

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

Dear <<First_name>> <<Last_name>>,

The University of Nebraska Medical Center (“UNMC”) takes the privacy and security of your information seriously. UNMC maintains computer software applications that support research studies, quality improvement projects, and public health activities. This letter relates to one of those applications, REDCap, that we believe contained your information. This information may have been collected directly from you by UNMC or UNMC may have received your information through a collaboration. Unfortunately, we recently learned that an unauthorized individual had access to REDCap and may have viewed your information. This letter explains what happened, what information was involved, what we are doing, and what you can do to help protect your information.

What happened. In February 2026, we learned that REDCap had a vulnerability that could allow an unauthorized person to gain remote access to the application. As soon as we learned of this issue, we took REDCap offline and began an investigation with privacy and cybersecurity partners. On February 18, 2026, the investigation determined that REDCap was subject to unauthorized access between September 20, 2023 and February 3, 2026. The investigation was unable to conclusively determine whether specific records stored in REDCap were viewed or taken. Out of an abundance of caution, we wanted to notify you of this incident.

What data was involved. The information that may have been involved varied by project and by individual. It may have included your name; Social Security number; identifiers such as date of birth, address, phone number, email address, and/or medical record number; and information created or collected in connection with a research study, such as clinical information, visit dates, diagnoses, medications, laboratory results, imaging or procedure information, questionnaire responses, or other health-related information.

What we are doing. We have secured the services of Experian® to offer you a complimentary <<b2b_text_2 (one/two)>>-year membership to Experian’s IdentityWorksSM. 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 completely free and enrolling in this program will not hurt your credit score. Additionally, to help prevent a similar incident from occurring in the future, we took REDCap offline as soon as we determined it was at risk, and began moving it to an updated version of REDCap that was released to address the vulnerability. This new version has enhanced logging and security controls enabled.

What you can do. While we do not have evidence that your information was actually viewed, taken, or misused, it is always a good idea to review statements you receive from your healthcare providers. If you see charges for services you do not recognize, you should contact the issuing provider immediately. For additional guidance on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary membership, please see the pages that follow this letter.

For more information. If you have questions, please call (844) 403-4589 Monday through Friday, 8:00 a.m. to 5:30 p.m., Central Time, excluding U.S. holidays.

Sincerely,

University of Nebraska Medical Center

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by <<b2b_text_6 (activation deadline)>> (Your code will not work after this date and enrollment must occur by no later than 11:59 pm)
2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE your activation code: <<Activation Code s_n>>

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 1-877-288-8057 by <<b2b_text_6 (activation deadline)>>. Be prepared to provide engagement number <<b2b_text_4 (Engagement #)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<b2b_text_3 (ONE/TWO)>>-YEAR EXPERIAN IDENTITYWORKS 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.
- **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 1-877-288-8057 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 1-877-288-8057.

**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, 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.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

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:

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

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.

The University of Nebraska Medical Center can be reached by mail at 42nd & Emile, Omaha, Nebraska 68198 or by phone at 402-559-4000.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 400 6th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: 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/

Massachusetts: Under Massachusetts 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: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York: 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: 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: This incident involves 0 individuals in Rhode Island. 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

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 NW, 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.