Data Notice

What Happened?

On April 1, 2026, Campbell University ("Campbell" or "we") discovered a security incident that affected one of our cloud-based data storage platforms. We immediately began an investigation and took steps to contain and remediate the situation including changing passwords, proactively taking the affected platform offline, working with the cloud-based provider to restore the platform from backups, notifying federal law enforcement, and engaging cybersecurity and privacy professionals to assist in our response. The investigation determined that there was unauthorized access to this Campbell system from March 31, 2026, to April 1, 2026. Thanks to our existing protections, the Incident was isolated to this single platform, and no other campus computer systems or data sources were impacted.

At this time, the investigation remains ongoing into the types of data ("Information") and identity of individuals who were affected by the Incident. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

What Information Was Involved?

Based on the findings of the investigation, the following types of information may have been impacted: name, address, date of birth, admission date, discharge date, death date, medical record number, provider or facility name, medical condition, diagnosis and/or treatment information, lab results, prescriptions and/or medications, personal history, mental health information, insurance/payment amount history information, date of service, payment card information, and/or any information on an individual that was created, used, or disclosed in the course of providing health care services, and Social Security number, driver's license or state identification number, passport number, student identification number, other government identification number, financial account information, debit/credit card information, health insurance information, medical information, individual taxpayer identification number, identity protection PIN issued by the IRS, parent's legal surname prior to marriage, digital signature, geolocation, and/or user name and access information for a non-financial account. Note that this describes general categories of information identified as present within the affected Campbell University system during the incident and includes categories that are not relevant to each individual whose information may have been present.

What We Are Doing.

We take this event and the security of Information in our care seriously. Upon becoming aware of the Incident, we immediately implemented measures to further strengthen the security of our systems and practices, including resetting identified passwords, setting up a new instance of the affected platform, reviewing and strengthening data access and local administrative policies, and implementing further technical safeguards on top of our existing protocols. After determining that an unauthorized actor gained access to our systems, we immediately began analyzing the information involved to confirm the identities of potentially affected individuals to notify them in a timely manner. Additionally, we are reporting the Incident to relevant government agencies.

What Can Impacted Individuals Do?

The investigation is ongoing and the full list of individuals who were affected is not yet known. However, out of an abundance of caution, we encourage individuals to remain attentive against potential identity theft and fraud, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. Presented below are steps that individuals can take to protect their personal information, including health and medical information.

We take this Incident and the security of information in our care seriously. If you have additional questions, you may call 910-893-1645 Monday through Friday from 8:30 AM to 5:00 PM ET (excluding U.S. holidays).

Steps You Can Take to Protect Your Personal Information

To obtain a free credit report, individuals may visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

Alternatively, affected individuals can contact the three (3) major credit reporting bureaus directly at the addresses below:

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 19022, https://www.transunion.com/data-breach-help, 1-833-799-5355

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

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.

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft pursuant to the Fair Credit Reporting Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) 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): (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth; (iv) current address and any previous addresses for the past five (5) years; and (v) any applicable incident report or complaint with a law enforcement agency or the Department 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.

FTC 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 FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. Contact information for the Consumer Response Center of the FTC is 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338) or www.ftc.gov/bcp/edu/microsites/idtheft/.

For North Carolina Residents: You may obtain information about preventing identity theft from the FTC (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400. You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.