Notice of Data Security Incident

Updated: April 11, 2025

Albany College of Pharmacy and Health Sciences (ACPHS) is committed to protecting the privacy and security of the personal information we maintain. We are making individuals aware of a data security incident involving unauthorized access to certain systems on our network. As part of the investigation, we engaged third-party cybersecurity professionals experienced in handling these types of incidents. Although we have no evidence of financial fraud or identity theft related to this data, in accordance with applicable law, we are making potentially affected individuals aware of the incident, resources, and steps that they may take to protect their personal information, should they feel it appropriate to do so.

Our investigation of the incident is ongoing. Once our investigation is complete, we will provide notice of the incident to the potentially impacted individuals.

What Happened? On or about September 14, 2024, ACPHS detected unusual activity on our network. Upon identifying this, ACPHS immediately took steps to remediate the incident and ensure the security of our systems, and commenced a thorough investigation. As part of this investigation, we have been working closely with external cybersecurity professionals experienced in handling these types of incidents. The investigation determined that certain systems on ACPHS's network were accessed by an unauthorized actor between approximately August 31, 2024, to September 14, 2024.

While our investigation into the incident is ongoing, we determined that the data on the affected systems contained a limited amount of personal information that may have been viewed or obtained by the unauthorized actor. We are completing the process of conducting an exhaustive review of the potentially impacted data to identify the individuals whose personal information may have been impacted. To date, we have no evidence of financial fraud or identity theft related to the impacted information. Nevertheless, once this review is complete, we will provide notice of the incident to the individuals whose personal information was potentially impacted.

What Information Was Involved? Based on our ongoing investigation and review, ACPHS determined that certain personal information was contained in the impacted data, including first and last name, date of birth, birth certificate, account number, routing number, security code, marriage certificate, mother's maiden name, digital signature, passport number, government identification number, Social Security number, taxpayer ID number, driver's license number, payment card number, payment card expiration date, alien registration number, username and password, health insurance information, medical information (including medical record number, mental or physical condition, diagnosis/treatment information, procedure type, provider name, prescription information, biometric data), and student information. The types of impacted information varied by individual.

What We Are Doing. The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed.

How Will Individuals Know If They Are Affected By This Incident? Once the investigation is complete, ACPHS is providing notice to individuals whose information was determined to be contained in the impacted data in accordance with our legal obligations and to the extent we have valid mailing addresses. If an individual does not receive a letter but would like to know if they are potentially affected, they may call 888-562-7067.

For More Information. ACPHS has established a toll-free call center to support our community with any further questions regarding this incident, please call our dedicated assistance line at 888-562-7067, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding holidays.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

Placing a Fraud Alert on Your Credit File.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.