Summit Healthcare – Notice of Breach of Patients' Protected Health Information

Posted: November 2, 2026

Summit Healthcare Association (SHA) values and respects the privacy and confidentiality of our patients' protected health information (PHI). Regrettably, this notice is to inform you of an incident that involves unauthorized access to some of that PHI by an individual who is no longer employed by SHA. We are providing this notice so that our patients and community understand what happened and the steps individuals can take.

What Happened?

On September 8, 2026, SHA determined, through investigation of a reported patient privacy concern, that between May 14, 2026 and September 4, 2026, a then-employee impermissibly accessed and viewed the PHI of patients listed on the Summit Healthcare Regional Medical Center's (SHRMC) ED and inpatient censuses, as well as some patients' medical records and other clinical information. Our investigation found the access was outside of the scope of the individual's job duties. SHA then reviewed access records to identify each patient whose information was accessed. To date, SHA's investigation has not identified any evidence that the information was further disclosed or misused.

What PHI was Involved?

Depending on the patient, the PHI involved included some or all of the following information: name, photo, date of birth, location(s) within facility, treating provider(s), date(s) of service, medical record and encounter numbers, health insurance information (such as member/group ID number or Medicaid/Medicare number), and medical records and/or clinical information (e.g., chief complaint, visit reason, history of present illness, vital signs, body measurements, medications, clinical notes, medical history, orders, and lab and imaging results). No financial information or social security numbers (SSNs) were accessed or viewed. Not all data elements were involved for every affected individual.

What is SHA Doing About It?

Upon learning of the concern, SHA promptly investigated and stopped the access. The individual is no longer employed by SHA. SHA is in the process of sending letters to affected patients by mail.

What Can You Do?

As noted above, SHA has not identified any evidence that the information was further disclosed or misused. However, if you are concerned about your personal information, you may wish to take the following steps to monitor and protect your personal information:

1. Review your health insurance statements. We recommend that you review the Explanation of Benefits statements you receive from your health insurer or Medicare/Medicaid. If you see services you did not receive, contact your insurer or plan right away.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled to one free copy of your credit report from each of the three major credit reporting companies every 12 months. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-

322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

3. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, you can place a fraud alert at one of the three major credit bureaus by phone and also via any bureau's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting 1-800-525-6285 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19016-2000 www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

*** Please Note: No one is allowed to place a fraud alert on your credit report except you.**

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. Report Suspected Identity Theft. If you believe someone is using your personal information, visit www.IdentityTheft.gov to report identity theft to the Federal Trade Commission's *Identity Theft Clearinghouse*, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261 and get assistance with a recovery plan. You can also report suspected online fraud to the Federal Bureau of Investigation's *Internet Crime Complaint Center* (IC3), at ic3.gov.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following resources:

- **Alaska Residents:** Alaska Department of Law at https://law.alaska.gov, 1031 W. 4th Avenue, Suite 200, Anchorage, AK. 99501-1994, (907) 269-5100.
- **Arizona Residents:** Arizona Attorney General's Office at https://www.azag.gov/consumer/data-breach/identity-theft, 2005 N. Central Avenue, Phoenix, Arizona 85004-2926, (602) 542-5025.

- **California Residents:** California Office of Privacy Protection www.oag.ca.gov/privacy, 1300 I Street, Sacramento, CA 95814, (800) 952-5225.
- **Florida Residents:** Office of Attorney General, https://www.myfloridalegal.com, Office of Attorney General, State of Florida, PL-01, The Capitol, Tallahassee, FL. 32399-1050, (850) 414-3300.
- **Nevada Residents:** Nevada Attorney General, https://ag.nv.gov, 100 N. Carson Street, Carson City, NV. 89701, (775) 684-1100 or (888) 434-9989.
- **New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- **New York Residents:** Office of the Attorney General: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov/, (800) 771-7755.
- **Texas Residents:** Texas Office of the Attorney General, https://www.texasattorneygeneral.gov, 300 W. 15th Street, Austin, TX 78701, (512) 463-2100.
- **All US Residents:**
    - Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.
    - Identity Theft Resource Center, https://www.idtheftcenter.org.

If you have any other questions or concerns, please contact our Privacy Officer, Natalie Roehlk, at (928) 537-6939 or via email: Natalie.Roehlk@summithealthcare.net.

SHA takes the privacy of our patients' information seriously, and we sincerely apologize for any concern this incident may cause.