Uintah Basin Healthcare

Uintah Basin Healthcare - Notice of Data Incident

May 10, 2023 – As previously reported by Uintah Basin Healthcare ("UBH"), we experienced a data security incident in November 2022. We now know that incident may have involved the personal and protected health information of certain individuals that received care services from UBH. This notification provides information about the incident and resources available to assist potentially impacted individuals.

What Happened. On November 7, 2022, UBH became aware of unusual activity on our network. In response, we immediately secured the environment and engaged a leading cybersecurity firm to assist with an investigation and determine whether sensitive, personal, or protected health information may have been affected

On or around April 7, 2023, UBH learned that the protected health information belonging to certain patients, specifically, those that received care with UBH between March 2012 and November 2022, may have been accessed or acquired without authorization during the course of this incident. UBH then worked diligently to evaluate potentially impacted information, confirm identities of potentially impacted individuals, and set up complimentary services being provided. That process was completed on April 10, 2023.

What Information Was Involved. The following protected health information may have been involved in the incident: name, date of birth, address, Social Security number, health insurance information, and certain clinical details including diagnosis/conditions, medications, test results, and procedure information.

Please note that UBH has no evidence that any potentially impacted information has been misused.

What UBH Is Doing. Data privacy and security are among UBH's highest priorities. UBH has taken steps to help prevent a similar incident from occurring in the future. In addition, UBH has provided notice of this incident to potentially impacted individuals. The notice that was provided included information about the incident and about steps that potentially impacted individuals can take to help protect their information. UBH has also established a toll-free call center to answer questions about the incident. Call center representatives are available Monday through Friday from 7:00 AM – 7:00 PM Mountain Time and can be reached at 1-888-567-0240.

What You Can Do. UBH encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanations of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors.

The privacy and security of all personal and protected health information is a top priority for UBH, and we deeply regret any inconvenience or concern this incident may cause.

UBH is also providing the following information to help those who want to know more about steps they can take to protect themselves and their personal and protected health information:

What steps can I take to protect my personal and protected health information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in your name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

How do I obtain a copy of my credit report?

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

How do I put a fraud alert on my account?

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

How do I put a security freeze on my credit reports?

You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; and (4) address. You may also be asked to provide other personal information such as your email address, 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, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove a freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	www.transunion.com

What should I do if my family member's information was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and TransUnion, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax	**Experian**	**TransUnion**
Equifax Information Services	Experian Information Services	Trans Union Information Services
P.O. Box 105169,	P.O. Box 9701	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

What should I do if my minor child's information is involved in the incident?

You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found above.