

Notice of Security Incident

Bacon County Health Services, Inc. and all other practices (“BCHS” or “we”) is issuing notice of an event that may involve personal and protected health information. While our investigation remains ongoing, we want to keep our community informed of this event so individuals may take steps to protect their information, should they feel it is appropriate to do so. BCHS reserves the right to update this page as needed as the investigation progresses.

What Happened?

On July 27, 2026, BCHS initially became aware of unusual activity within its internal network. Immediate action was taken to secure our network and to ensure that patient care was not disrupted. Additionally, BCHS promptly launched an investigation with assistance from cybersecurity specialists to determine the nature and scope of the activity. The investigation determined that the network had been accessed by an unknown actor between July 10, 2026 and July 27, 2026, and during this time, files were copied and potentially viewed.

What Is BCHS Doing?

The privacy of patient information is one of our top priorities. We reported the incident to law enforcement and notified the U.S. Department of Health and Human Services. BCHS is currently conducting a comprehensive and thorough review of the contents of the potentially affected files to identify any personal and protected health information contained therein and to whom that information relates. Once our review is complete, we will move as quickly as possible to directly notify individuals whose information is present in the affected files and provide detail about the types of information at issue for each individual.

What Information Was Involved?

At this stage, our review of potentially impacted data remains ongoing, and it is too early to tell what specific information was involved.

What Can You Do Now?

To date, we are not aware of any reports of identity fraud or fraudulent activity involving your information as a result of this incident. However, it is always prudent to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and to report any suspicious activity promptly to your insurance company, health care provider, or financial institution.

Frequently Asked Questions

What Types of Data Were Affected?

The investigation remains on going. When we learn what information was involved, and to whom the information belongs, affected individuals will receive a notice letter (or will otherwise be notified in accordance with law).

How Will I Be Notified If My Information Was Involved?

At the conclusion of our data review, BCHS will mail a notice letter to individuals whose information is determined to be in the potentially affected files and for whom we have a valid mailing address. Please note that because the review is still ongoing, we will not be able to confirm if any individual information is affected at this time until the review is complete.

I Have More Questions About this Event.

While our investigation remains ongoing, we understand you may have additional questions. BCHS will update this page as needed as the investigation progresses. In the meantime, we are fully committed to maintaining your trust throughout this process. For more information or further assistance please call Alissa Peacock at 912-632-8961 extension 1072.

What Can I Do to Protect my Information?

As a best practice, BCHS encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their accounts, explanations of benefits, and credit reports for suspicious activity, and to report any suspicious activity to the affiliated institutions immediately. As an added precaution, individuals can also review the steps you can take to protect against the possibility of identity theft and fraud below.

Steps You Can Take to Protect Your Information

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;

5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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.