

NOTICE OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION AND PERSONAL INFORMATION

Cornerstone Behavioral Healthcare (“Cornerstone”) is issuing this notice pursuant to the Breach Notification Rule of the Health Insurance Portability and Accountability Act (HIPAA) and Maine’s Notice of Risk to Personal Data Act.

On May 26, 2026, Cornerstone discovered that a breach of the security of certain PHI that Cornerstone maintains occurred as a result of a ransomware attack. This ransomware attack was initiated on the same day it was discovered, and any access the ransomware attackers had to Cornerstone’s systems was suspended within an hour of discovery. Ransomware is a type of malicious software that attempts to deny access to data. In this case, the ransomware was encrypting Cornerstone’s data so that Cornerstone could not access it. The ransomware included a demand that Cornerstone pay a ransom to regain access to its data. Cornerstone did not pay the ransom and was able to stop the attack and restore its electronic data. Cornerstone believes that less than 10% of the data in the affected computers and servers may have been encrypted by the ransomware attackers before Cornerstone was able to quickly power them down upon discovery of the attack.

Cornerstone undertook a prompt investigation of the incident and has determined that the following types of PHI and/or personal information concerning 2,830 individuals may have been compromised as a result of this incident, including: names, addresses, other contact information, dates of birth, health care information, substance use disorder treatment information, insurance/MaineCare information, and social security numbers. On July 22, 2026, Cornerstone’s continued investigation of the ransomware incident revealed that a log of appointment reminders for an additional 12,000 individuals may have been viewed or accessed during the ransomware attack. This log included patient names, dates of birth, appointment times, and reminders of documentation due, and Cornerstone is investigating whether any additional PHI or personal information was involved with respect to these 12,000 individuals.

Cornerstone has taken the following measures to investigate this breach, to mitigate the harm to persons affected by the breach, and to protect against any further breaches:

- Cornerstone’s leadership and information technology employees investigated the scope of the attack and promptly restored the affected data.
- Cornerstone wiped the affected computers and purchased new computers for its staff to use going forward.
- Cornerstone also reviewed its systems, policies, and procedures and implemented additional security measures to reduce the likelihood of an attack like this from occurring in the future. These measures included implementing extra layers of security for our servers and providing special training for our employees on ransomware.

Cornerstone is also notifying all affected individuals, and is recommending that they take the following additional steps to protect themselves from potential harm resulting from this breach:

1. Call the toll-free numbers or go to the websites of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge:

Equifax

Toll-Free Number: (800) 525-6285

Website: <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Experian

Toll-Free Number: (888) 397-3742

Website: <https://www.experian.com/fraud/center.html>

TransUnion

Toll-Free Number: (800) 680-7289

Website: <https://www.transunion.com/fraud-alerts>

2. Order your credit reports. By establishing a fraud alert, you will receive information that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as accounts you did not open.

3. Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

4. Closely monitor your bank statements and other financial information. If you believe that fraudulent activity is occurring, immediately contact your financial institutions.

5. When you file your federal income tax return you should also complete and attach Form 14039, the Identity Theft Affidavit. For assistance or more information, you may call the IRS at (800) 908-4490.

Cornerstone is also notifying the Secretary of the United States Department of Health and Human Services of this incident in compliance with its obligations under the HIPAA Breach Notification regulations at 45 C.F.R. §164.408.

Affected individuals with questions concerning this incident should contact Cornerstone at:

Cornerstone Behavioral Healthcare

Attention: Privacy Officer

157 Park Street, #5

Bangor, Maine 04401

Tel.: 207-992-0410

Email: privacyofficer@cornerstonebhc.com

Website : <https://cornerstonebhc.com/>

Cornerstone deeply regrets that this incident occurred and wants to assure affected individuals and members of the public that we take this incident and the privacy of the information we maintain about individuals very seriously and are working to ensure that this sort of incident does not occur again.