Website Notice

MedImpact values and respects the privacy and security of personal information, which is why it is providing notice of a recent cybersecurity incident that may have involved certain information associated with individuals who are or were members of pharmacy benefit plans administered by MedImpact and/or Elixir Solutions. This notice describes the measures MedImpact has taken since the incident and steps impacted individuals can take to further protect their personal information.

What Happened?

On October 18, 2025, MedImpact identified unauthorized activity within certain systems in its environment. MedImpact took immediate action after learning of the incident to secure the affected systems and launched an investigation, including working with outside cybersecurity experts to determine the source of the activity and potential impact on MedImpact's network. As part of that investigation, MedImpact conducted a detailed review of potentially impacted data.

On July 17, 2026, MedImpact finalized the investigation and determined that certain data relating to some individuals was included within the set of potentially impacted data evaluated in connection with the incident. On August 13, 2026, MedImpact notified its clients of the incident. On September 25, 2026, MedImpact began mailing notices to potentially impacted individuals on behalf of its clients.

What Information Was Involved?

The information involved varied by individual. Based on the review, the information may have included first and last name and one or more of the following: address, date of birth and subscriber number; limited health-related information, including prescription information, information about treatment (including the date of service, location, or provider name); insurance identification numbers; and, in limited instances, Social Security numbers.

What We Are Doing

MedImpact takes the protection of personal information very seriously. MedImpact took steps to launch an investigation immediately after identifying the incident, enlisted cybersecurity experts to assist in the investigation, and notified law enforcement. MedImpact also promptly implemented additional technological safeguards to minimize the possibility of an incident like this occurring in the future. MedImpact is attempting to notify potentially impacted individuals by letter when a mailing address is available. Where an individual's Social Security number was potentially impacted, MedImpact is offering complimentary credit monitoring and identity theft protection services at no cost to the individual.

What You Can Do.

Although MedImpact is not aware of any misuse of personal information resulting from this incident, as a best practice, we encourage all individuals to remain vigilant against incidents of identity theft and fraud, to review all claims information from a health insurance provider, and to monitor credit reports and financial statements for suspicious activity. You can set up free fraud alerts with nationwide credit bureaus, Equifax, Experian, and TransUnion. For additional information, see the "Additional Financial Information" section below.

For More Information

MedImpact set up a dedicated, toll-free call center that will be available starting on September 22, 2026, to answer questions related to this incident. Individuals who believe they may have been impacted or who would like additional information may call (844) 958-8925, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major holidays).

Additional Financial Information

The Federal Trade Commission (FTC) has released suggestions for individuals who are concerned about financial crimes. We have provided that information here. The FTC recommends that you place a free fraud

alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: www.equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: www.experian.com/help or 1-888-397-3742

TransUnion: http://www.transunion.com/credit-help or 1-888-397-3742

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at www.IdentityTheft.gov to report the identity theft and get recovery steps. The FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also visit FTC's website, www.IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft.