Notice of Data Incident

Med Atlantic, Inc. ("MedAtlantic") has detected a data security incident on November 10, 2025. MedAtlantic provides services to regional urology providers including Virginia Urology. This compromise could have permitted an unauthorized individual to access personal health information. We immediately stopped the compromise, secured this data, and took steps to mitigate. We brought in third-party experts to investigate and that investigation concluded on December 1, 2025. MedAtlantic then worked with medical providers to identify and notify potentially impacted individuals. Unfortunately, these types of incidents have become increasingly common, and organizations of all sizes are affected.

The investigation determined that someone could have had access to your health information related to services received at MedAtlantic. Personal or health information that could have been compromised vary by individual.

We take information privacy seriously and will continue to strengthen our data security to prevent a similar event from occurring in the future. We are also focused on improving our data protection through additional awareness training and updating our procedures. MedAtlantic notified the Office for Civil Rights and law enforcement regarding this incident.

Additionally, out of an abundance of caution, we have secured the services of Epiq - Privacy Solutions ID to provide complimentary identity monitoring, identity restoration, and identity theft insurance should the need arise.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Please review the following additional information for further steps to safeguard your personal information.

Please know that MedAtlantic and Virginia Urology value the protection and privacy of your personal and health information, and we understand the concern and inconvenience this incident may cause. If you have any questions, call 888-367-0212 between 6:00 AM and 6:00 PM PT, Monday through Friday, excluding holidays.

Steps Individuals Can Take to Protect Personal Information

Monitoring: You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity. You can report suspicious activity to financial institutions or law enforcement.

Fraud Alert: You can place fraud alerts with the three major credit bureaus by phone and online as set forth below with Equifax, TransUnion, or Experian. 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. Initial fraud alerts last for one year. Victims of identity theft can get an extended fraud alert for seven years.

Credit Report: Consumers are also entitled to one free credit report annually from each of the three credit reporting bureaus. To order your free credit report: visit www.annualcreditreport.com; call, toll-free, 1-877-322-8228; or mail a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: 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, regular stamped mail, or by following the instructions found at the websites listed below. The following information may need to be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current and addresses for the past five years; (5) proof of address; (6) Social Security Card, pay stub, or W2; or (7) government-issued identification card. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**Equifax**	**TransUnion**
1-888-397-3742	1-800-349-9960	1-888-909-8872
www.experian.com/help/	www.equifax.com/personal/credit-report-services/	www.transunion.com/credit-help
Fraud Alert P.O. Box 9554 Allen, TX 75013	Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Fraud Alert P.O. Box 2000 Chester, PA 19016
Credit Freeze P.O. Box 9554, Allen, TX 75013	Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Credit Freeze P.O. Box 160, Woodlyn, PA 19094

Implementing an Identity Protection PIN (IP PIN) with the IRS: To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don’t already have an account on IRS.gov, you must register and validate your identity. Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. Some items to consider when obtaining an IP PIN with the IRS: (1) an IP PIN is valid for one calendar year; (2) a new IP PIN is generated each year for your account; (3) logging back into the Get an IP PIN tool, will display your current IP PIN; and (4) an IP PIN must be used when filing any federal tax returns during the year including prior year returns.

Federal Trade Commission: More information can be obtained by contacting the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft