Medtronic

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<Date>

Re: Notice of Data Breach

Dear <<Name>>:

We are writing to notify you that Medtronic Inc. ("Medtronic") was the victim of a cybersecurity incident that may have involved certain personal information related to you. We are contacting you to explain the circumstances of the incident, the types of information that may have been involved, and steps you can take to further safeguard your information, should you feel it appropriate to do so. Data privacy and security are a top priority for Medtronic. We regret any concern this may cause you.

What Happened? On April 15, 2026, Medtronic became aware of unusual activity on certain corporate IT systems. Medtronic launched an investigation with the assistance of leading third-party cybersecurity experts to determine the impact and scope of the incident. The investigation determined that from April 13 to April 19, 2026, an unauthorized actor accessed certain Medtronic corporate IT systems. With the assistance of data review specialists, we have been working diligently to determine the types of information that may have been subject to unauthorized activity and to whom they relate.

What Information Was Involved? As a patient with a Medtronic medical device, our company collects data related to you in order to provide important product-related updates and to meet our legal obligations. The investigation to date has determined that the following types of information may have been impacted: name, contact information, date of birth, Social Security number, and health-related information. We have no evidence that any of that information was posted publicly or exposed on the Internet.

Your Medtronic Device Remains Safe. We understand that you may have questions about the safety or performance of your Medtronic device. Based on our investigation, this incident did not impact the ability of any Medtronic device to operate safely and deliver intended therapy.

What We Are Doing. Medtronic is committed to and takes very seriously our responsibility to safeguard all data entrusted to us. As part of our ongoing commitment to the security of personal information in its care, Medtronic has implemented additional safeguards and continues to work with third-party cybersecurity experts to identify opportunities to further strengthen the security of its systems. Medtronic has also worked with law enforcement and is notifying relevant regulatory authorities.

In addition, we are offering you access to 24 months of complimentary credit monitoring, dark web monitoring (monitoring certain online sources for publication of personal information), and identity theft restoration services through Epiq. Details on the service and instructions for enrollment can be found in the enclosed *Epiq – Privacy Solutions ID*.

What You Can Do. You can enroll in the complimentary credit monitoring, dark web monitoring, and identity theft restoration services that Medtronic is offering. In addition to enrolling in this complimentary service, we recommend that, out of an abundance of caution, you remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors.

You should also be cautious of unexpected communications, including emails, text messages or phone calls, requesting personal information. Please review the enclosed *Steps You Can Take to Protect Your Personal Information* for additional guidance.

For More Information. We understand that you may have additional questions that are not addressed in this letter. Please call 888-289-6806 Monday through Friday, 9 AM to 9 PM ET with any questions you may have.

Sincerely,

Medtronic Inc.

<<Full Name>>
Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<ENROLLMENT DEADLINE>>
Coverage Length: 24 Months

Epiq - Privacy Solutions ID

3B Credit Monitoring + Medical Monitoring

How To Enroll:

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

Product Features:

3-Bureau Credit Monitoring with Alerts

Monitors your credit file(s) with each of the 3 Credit Bureaus for key changes, with alerts such as credit inquiries, new accounts, and public records.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring

Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring

Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection

3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance[1]

Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT[1]

Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

Healthcare Insurance Plan ID Monitoring & Medicare Beneficiary Identifier ID Monitoring

Monitors the dark web for exposed registered healthcare, dental, vision, and prescription plan IDs. Monitors the dark web for exposed Medicare Beneficiary Identifier ID numbers.

Medical Record Number Monitoring

Alerts when a Medical Record Number has been detected on the dark web, which could potentially expose permanent medical and health records from providers, hospitals, and urgent care centers.

International Classification of Disease Monitoring

Monitors the dark web for exposed medical information - and notifies users if their PII is exposed along with ICD (disease) codes.

National Provider Identifier Monitoring

Monitor NPI numbers (for healthcare professionals) on the dark web to detect unauthorized usage or exposures.

Health Savings Account Monitoring

Monitors the dark web for exposed HSA account information.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring + Medical Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Help Protect Your Personal Information / Other Important Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Place a Security Freeze

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 380	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-378-4329
www.experian.com/freeze/center.html	www.transunion.com/ credit-freeze	www.equifax.com/personal/credit-report-services/credit-freeze/

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Place a Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-916-8800	1-888-378-4329
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Additional Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Iowa Residents: State law advises you to report any suspected identity theft to local law enforcement or the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General and FTC about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us. The information for the FTC is listed above.

For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA").

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of
Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, Consumer Protection Division, 90001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000, www.ncdoj.gov.

For Oregon Residents: State law advises you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903; (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services. The investigation to date has identified approximately 12,054 potentially impacted Rhode Island residents.

Washington, D.C. Residents: You can obtain information about avoiding identity theft from the Office of Attorney General for the District of Columbia. You can contact the Office of Attorney General for the District of Columbia at: 400 6th Street NW, Washington, D.C. 20001; 1-202-727-3400; https://oag.dc.gov.