Medtronic

Diabetes
18000 Devonshire St
City, ST 12345
USA
www.medtronicdiabetes.com

20286

To Enroll, Please Call:
[TFN]
Or Visit:
https://response.idx.us/customending

https://app.idx.us/account-creation/protect

Enrollment Code: [XXXXXXXX]

Dear [Name]:

We are sending this letter to you as part of our commitment to our customers' privacy. We take customer privacy very seriously, and it is important to us that you are aware of an incident we learned of on March 12, 2020, which may have compromised your sensitive personal information.

What happened?

On March 12, 2020, the computer, phone, and iPad of an employee was taken and accessed by an unauthorized individual for a short period of time. Upon learning of the incident, Medtronic took immediate action to investigate and retrieve the devices back. In the process, we determined that the individual may have accessed or taken screenshots of information that could have included patient data. Our investigation has revealed no evidence of any compromise of our systems. However, we are unable to confirm whether the individual misappropriated or accessed patient information. As such, out of an abundance of caution, and because of the sensitive nature of this information, we are notifying all customers whose sensitive personal or financial information might have been accessed by this individual.

What information was impacted?

The information at issue may have included your name, address, phone number, email, date of birth, and social security number.

What are we doing to help?

We are alerting you and others who may have been impacted so that you can take steps to protect yourself. As a precaution, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. Medtronic is not affiliated in any way with IDX; however, their services are highly recommended. With this protection, IDX has tools to help you resolve issues if your identity is compromised.

Instructions for enrolling in credit monitoring:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling [TFN] or going to https://response.idx.us/customending / https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is [Enrollment Deadline].

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

What are we doing?

Medtronic began an investigation immediately upon learning of this incident, including a forensic investigation of the employee's computer, phone, iPad, and our systems. The employee's system access was suspended, and employment has been terminated.

In addition to the steps described above, we have also contacted the Department of Health and Human Services, and the applicable state agencies regarding this incident. In addition, we are continuing our investigation, reviewing our policies and procedures, and implementing further training with our employees to avoid any future incidents.

What can you do?

Monitor your accounts for any unusual activity. You may also wish to consider contacting the three credit reporting bureaus and requesting a fraud alert or a credit freeze be placed on your account. Contact information and a guide for how to make these requests appears on the following pages.

You are also entitled to a free credit report every year from each of these agencies. You can request the report at www.annualcreditreport.com.

We understand that this may cause concern and inconvenience you. We sincerely apologize and regret that this situation has occurred. Medtronic is committed to protecting your personal health information and we want to assure you that we are dedicated to ensuring that this does not happen again in the future.

Please do not hesitate to contact IDX with any questions about this incident, or for additional information on steps to take as a result of this incident, at [TFN].

Sincerely,

Mark Grant

VP Americas, Diabetes

Medtronic

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://response.idx.us/customending / https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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.

Medtronic

Diabetes
18000 Devonshire St
City, ST 12345
USA
www.medtronicdiabetes.com

To Enroll, Please Call:
[TFN]
Or Visit:
https://app.myidcare.com/account-creation/protect

Enrollment Code: [XXXXXXXX]

Dear Parent or Guardian of <<Minor First Name>> <<Minor Last Name>>:

We are sending this letter to you as part of our commitment to our customers' privacy. We take customer privacy very seriously, and it is important to us that you are aware of an incident we learned of on March 12, 2020, which may have compromised your minor's sensitive personal information.

What happened?

On March 12, 2020, the computer, phone, and iPad of an employee was taken and accessed by an unauthorized individual for a short period of time. Upon learning of the incident, Medtronic took immediate action to investigate and retrieve the devices back. In the process, we determined that the individual may have accessed or taken screenshots of information that could have included patient data. Our investigation has revealed no evidence of any compromise of our systems. However, we are unable to confirm whether the individual misappropriated or accessed patient information. Out of an abundance of caution, and because of the sensitive nature of this information, we are notifying all customers whose sensitive personal or financial information might have been accessed by this individual.

What information was impacted?

The information at issue may have included your minor's name, address, phone number, email, date of birth, and social security number.

What are we doing to help?

We are alerting you and others who may have been impacted so that you can take steps to protect your minor. As a precaution, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. Medtronic is not affiliated in any way with IDX; however, their services are highly recommended. With this protection, IDX will help you resolve issues if your identity is compromised.

Instructions for enrolling in credit monitoring:

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling [TFN] or going to https://response.idx.us/customending / https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is [Enrollment Deadline].

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

What Are We Doing?

Medtronic began an investigation immediately upon learning of this incident, including a forensic investigation of the employee's computer, phone, iPad and our systems. The employee's system access was suspended, and employment has been terminated.

In addition to the steps described above, we have also contacted the Department of Health and Human Services, and the applicable state agencies regarding this incident. In addition, we are continuing our investigation, reviewing our policies and procedures, and implementing further training with our employees to avoid any future incidents.

What Can You Do?

Monitor your minor's accounts for any unusual activity. You may also wish to consider contacting the three credit reporting bureaus and requesting a fraud alert or a credit freeze be placed on your minor's account. Contact information and a guide for how to make these requests appears on the following pages.

You are also entitled to a free credit report every year from each of these agencies. You can request the report at www.annualcreditreport.com.

We understand that this may cause concern and inconvenience you. We sincerely apologize and regret that this situation has occurred. Medtronic is committed to protecting your personal health information and we want to assure you that we are dedicated to ensuring that this does not happen again in the future.

Please do not hesitate to contact IDX with any questions about this incident, or for additional information on steps to take as a result of this incident, at [TFN].

Sincerely,

Mark Grant

VP Americas, Diabetes

Medtronic

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://response.idx.us/customending / https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive

confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

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.