



November 5, 2013

ATTORNEY GENERAL
2013 NOV 12 AM 11:47

The Honorable Thomas J. Miller
1305 E. Walnut Street
Des Moines IA 50319
Fax: (515) 281-4209

Dear Mr. Attorney General:

DaVita, a division of DaVita HealthCare Partners (“DaVita”), writes to inform you about a security incident that impacts individuals within your state or jurisdiction. Specifically, we discovered that on September 6, 2013 a laptop was stolen from an employee’s vehicle. Although DaVita maintains a company-wide program and policy requiring encryption of laptop computers, we discovered that the encryption technology on this particular device had been unintentionally deactivated. The computer was, however, password protected. After learning of the theft, the incident was reported to law enforcement.

Based on our investigation, we have determined that information about DaVita patients, employees, and third-party vendors was included on the laptop. The information included individual names, clinical diagnoses (*e.g.*, end stage renal disease), insurance carrier name, claims payment data, dialysis treatment information, and in some instances, Social Security numbers. We believe at this point that a small amount of non-patient credit card numbers may have also been stored on the laptop and are continuing to investigate. We have cancelled any DaVita-issued credit cards that have been identified on the laptop.

The information of approximately 9 individuals in your state or jurisdiction was contained on the laptop.

There is no indication that the information has been misused in any way or was taken for the purposes of committing identity theft or causing other financial harm to the individuals. Nevertheless, in order to protect any affected individuals we have retained ID Experts to provide identify theft protection services, which includes free credit monitoring for one year to all impacted individuals who choose to enroll, along with identity recovery assistance and \$20,000 insurance for reimbursement of expenses if identity theft occurs. For any affected patients that are minors, the package includes recovery assistance with ID Experts and \$20,000 insurance for reimbursement of expenses if identity theft occurs. Additionally, we have a dedicated call center to address any questions or concerns of those affected.

We take very seriously our responsibility to protect the privacy of information. The affected individuals residing in your state or jurisdiction will be sent one of the attached written notifications on November 5, 2013. The version they receive depends upon whether or not the individual’s Social Security Number was contained in the laptop. In all material aspects, the letters are identical other than the description of the types of information at issue. We will also be notifying the three major credit reporting agencies.



Sincerely,

A handwritten signature in blue ink that reads "Alan Cullop".

Alan Cullop
Chief Security Officer

A handwritten signature in blue ink that reads "Betsy McCubrey".

Betsy McCubrey
Chief Privacy Officer

Attachments



November 5, 2013

Dear DaVita Patient:

We regret to inform you that on September 6, 2013 a laptop was stolen from a teammate's (employee's) vehicle. Although DaVita maintains a company-wide program and policy requiring encryption of laptop computers, we discovered that the encryption technology on this particular device had been unintentionally deactivated.

Based on our investigation, we have determined that personal information about you was included on the laptop. The information included details such as your name, clinical diagnoses (e.g., end stage renal disease), insurance carrier name, claims payment data, dialysis treatment information, and Social Security number.

At DaVita, we take our responsibility to protect your information very seriously. We maintain extensive security and privacy programs. The laptop in question was password protected, and the theft was reported to law enforcement. We have no evidence that your data has been accessed or used. Nonetheless, out of an abundance of caution and to ensure that you are protected, we recommend that you remain vigilant for incidents of potential fraud and monitor your financial account statements and credit reports.

There are several sources of information that discuss ways to prevent identity theft. Those sources include the FTC and the three major credit reporting agencies. Below is the contact information for these agencies where you can obtain additional information and/or free credit reports, as applicable:

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580

www.ftc.gov

1-877-438-4338; TTY: 1-866-653-4261

TransUnion, LLC

PO Box 2000
Chester, PA 19022

www.tuc.com

1-800-888-4213

Equifax

PO Box 9740256
Atlanta, GA 30374

www.equifax.com

1-800-655-1111

Experian

PO Box 9701
Allen, TX 75013

www.experian.com

1-888-397-3742



To further ensure you are protected, we are offering you one year of credit monitoring, identity recovery assistance and identity theft insurance through idexperts® at no charge to you. We encourage you to take advantage of the services available to you. **To activate your free credit monitoring, please call the number below and it will be set up for you.**

We sincerely apologize for any inconvenience or concern this incident may cause you. DaVita has reviewed its encryption practices and implemented additional safeguards to protect against any future instances of non-compliance with our encryption policies and procedures.

If you have questions regarding this incident, please call 1-866-797-3792 toll free Monday through Friday, 9:00 AM to 9:00 PM EST.

Sincerely,

A handwritten signature in blue ink that reads "Alan Cullop".

Alan Cullop
Chief Security Officer

A handwritten signature in blue ink that reads "Betsy McCubrey".

Betsy McCubrey
Chief Privacy Officer

Enclosure (1)



November 5, 2013

Dear DaVita Patient:

We regret to inform you that on September 6, 2013 a laptop was stolen from a teammate's (employee's) vehicle. Although DaVita maintains a company-wide program and policy requiring encryption of laptop computers, we discovered that the encryption technology on this particular device had been unintentionally deactivated.

Based on our investigation, we have determined that personal information about you was included on the laptop. The information included details such as your name, clinical diagnoses (e.g., end stage renal disease), insurance carrier name, claims payment data, and dialysis treatment information.

The laptop did not contain your Social Security number, Drivers' License number, State Identification Card number, or credit card account information.

At DaVita, we take our responsibility to protect your information very seriously. We maintain extensive security and privacy programs. The laptop in question was password protected, and the theft was reported to law enforcement. We have no evidence that your data has been accessed or used. Nonetheless, out of an abundance of caution and to ensure that you are protected, we are offering you one year of credit monitoring through idexperts® at no charge to you. Please call the toll free number below for assistance activating your credit monitoring service.

We sincerely apologize for any inconvenience or concern this incident may cause you. DaVita has reviewed its encryption practices and implemented additional safeguards to protect against any future instances of non-compliance with our encryption policies and procedures.

If you have questions regarding this incident, please call 1-866-797-3792 toll free Monday through Friday, 9:00 AM to 9:00 PM EST.

Sincerely,

A handwritten signature in blue ink, appearing to read "Alan Cullop".

Alan Cullop
Chief Security Officer

A handwritten signature in blue ink, appearing to read "Betsy McCubrey".

Betsy McCubrey
Chief Privacy Officer

Enclosure (1)

Recommended Steps to Help Protect Your Identity

Please Note: No one is allowed to place a fraud alert on your credit report except you; please follow the instructions below to place the alert.

1. Telephone. Contact 1-866-797-3792 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. 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.

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.

3. Place Fraud Alerts with the three credit bureaus. 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
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
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.

4. Security Freeze. By placing a 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 in writing 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. The cost of placing the freeze varies by the state you live in and for each credit reporting agency. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them