



**STATE OF WASHINGTON
HEALTH CARE AUTHORITY**

626 8th Avenue, SE • P.O. Box 42700 • Olympia, Washington 98504-42700

February 9, 2016

The Honorable Bob Ferguson
Attorney General for the State of Washington
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

SUBJECT: Formal Notice Pursuant to RCW 42.56.590

Dear Attorney General Ferguson:

Pursuant to RCW 42.56.590, the Washington State Health Care Authority (HCA) is providing formal notice of an unauthorized disclosure of protected information concerning Apple Health (Medicaid) beneficiaries. The following kinds of information were disclosed:

- Name
- Address and phone number
- Social Security number
- Date of birth
- Apple Health ID
- Medical procedure information
- Medical diagnosis information

Although HCA has no evidence that any Apple Health information was inappropriately used, its investigation and risk assessment have concluded that a report to your office is statutorily required. This unauthorized disclosure of protected information relates to approximately 91,187 Medicaid beneficiaries.

Description of Incident

Between November 15, 2013, and December 24, 2015, an HCA employee emailed spreadsheets containing Apple Health client information to another state employee who should not have received the information. While both the HCA employee and the recipient of the emails assert that the information was shared only for work purposes and was not used inappropriately in any manner, HCA cannot be sure that this is the case. HCA became aware of the potential unauthorized disclosure of Apple Health information on about December 16, 2015, and the agency began taking immediate steps to assess and investigate the matter.

What HCA Has Done in Response to the Incident

Upon discovery of this incident, HCA promptly took a number of steps including:

- Investigating how the information was transferred and used.
- Taking possession of all information that was sent by the HCA employee and received by the other state employee.
- Conducting separate interviews with both employees to understand the circumstances surrounding the exchange of information and to determine what they did with the information. Both employees assert that the exchange of information occurred because the HCA employee needed technical assistance with spreadsheets, and that the information was not used for any additional unauthorized purposes or forwarded to any other unauthorized recipients.
- Terminating the employment of the HCA staff involved in the incident.
- Reminding all HCA employees as to the importance of protecting private health and personal information.
- Planning additional training for our staff to address this specific issue.
- Notifying the appropriate federal officials for further investigation and potential criminal review.

What HCA Is Doing to Protect Apple Health Beneficiaries

A copy of the individual notices being sent to adult, minor, and deceased beneficiaries is attached to this letter. These notices provide detailed information about what the HCA is doing to protect Apple Health beneficiaries. In summary, HCA is working closely with Experian® to offer the following no-cost protections for one year:

- ProtectMyID® Alert for adults. This product helps detect possible misuse of personal information and provides superior protection and support focused on immediate identification and resolution of identity theft.
- FamilySecure® for the parent or guardian of any minors. This product monitors Experian credit reports and provides notification of key changes that could signal identify theft.

HCA has also provided a list of additional actions beneficiaries can take to protect themselves. Finally, beneficiaries have access to an Incident Response Line to address any questions they may have about the incident. The Incident Response Line can be accessed at: 1-877-866-9702.

The Honorable Bob Ferguson
Attorney General for the State of Washington
Page 3

Should you or any representatives from your office have questions or need further information, please don't hesitate to contact *Steve Dotson, Enterprise Risk Manager*, at 360-725-0444 or via email at steve.dotson@hca.wa.gov.

Very truly yours,



Steve Dotson
Enterprise Risk Manager
Division of Legal Services
Enterprise Risk Management Office

Enclosures

By email (SecurityBreach@atg.wa.gov)

cc: Executive Leadership Team (HCA)
Dennis Martin, Administrator of the Office of Legislative Affairs (HCA)
George Taylor, Privacy Officer (HCA)
Catherine George, Special Assistant to the Chief Operations Officer (HCA)
Angela Coats McCarthy, Assistant Attorney General
Matthew King, Assistant Attorney General



**STATE OF WASHINGTON
HEALTH CARE AUTHORITY**

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name1>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

SUBJECT: Notification Regarding Your Protected Health Information

The Washington State Health Care Authority (HCA) is sending this letter to you to make sure you are made aware of an incident resulting in the unauthorized disclosure of some of your Apple Health (Medicaid) information by an individual employee of HCA. We have learned that the following kinds of information were disclosed—some or all of which may apply to you:

- Name
- Address and phone number
- Social Security number
- Date of birth
- Apple Health ID
- Medical procedure information
- Medical diagnosis information

Although we have no evidence that your Apple Health information was inappropriately used, we need to inform you of this incident in writing. We also want to describe the steps we are taking to respond to this incident and outline the additional steps you can take to protect yourself from any potential harm.

Description of Incident

Between November 15, 2013, and December 24, 2015, an HCA employee emailed spreadsheets containing Apple Health client information to another state employee who should not have received the information. While both the HCA employee and the recipient of the emails assert that the information was shared only for work purposes and was not used inappropriately in any manner, we cannot be sure that this is the case. HCA became aware of the potential unauthorized disclosure of some of your Apple Health information on about December 16, 2015, and the agency began taking immediate steps to assess and investigate the matter.

What We Have Done in Response to the Incident

Upon discovery of this incident, HCA promptly took a number of steps including:

- Investigating how the information was transferred and used.
- Taking possession of all information that was sent by the HCA employee and received by the other state employee.
- Conducting separate interviews with both employees to understand the circumstances surrounding the exchange of information and to determine what they did with the information. Both employees assert that the exchange of information occurred because the HCA employee needed technical assistance with spreadsheets and that the information was not used for any additional unauthorized purposes or forwarded to any other unauthorized recipients.
- Terminating the employment of the HCA staff involved in the incident.

- Reminding all HCA employees as to the importance of protecting private health and personal information.
- Planning additional training for our staff to address this specific issue.
- Notifying the appropriate federal officials for further investigation and potential criminal review.

What We Are Doing to Protect Your Information

To help protect your identity, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE that you enroll by: April 30, 2016 (Your code will not work after this date.)
2. VISIT the ProtectMyID web site to enroll: www.protectmyid.com/redeem
3. PROVIDE Your activation code: <<Code>>

If you have questions or need an alternative to enrolling online, please call 1-877-288-8057 and provide engagement number: **PC98985**.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-288-8057.

HCA has also set up an **Incident Response Line** to address any questions you may have about this Notice or the incident. Please contact the **Incident Response Line** at: 1-877-866-9702.

What You Can Do to Protect Your Information

There are additional actions you can consider taking to reduce the chances of identity theft or fraud. Please refer to the final page of this Notice for additional information.

HCA takes our role of safeguarding your personal information and using it in an appropriate manner very seriously. We are committed to protecting the confidentiality of our clients' information and apologize for the concern this incident may have caused. We assure you that we are doing everything we can to prevent future incidents.

Additional Actions to Help Reduce your Chances of Identity Theft or Fraud

Place a 90-day Fraud Alert on your Credit File

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
1-800-525-6285
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

Place a Security Freeze on your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

Order your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

Obtain more Information about Identity Theft and ways to Protect Yourself.

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.
- The Washington State Attorney General's Office has information at:
 - www.atg.wa.gov/guardit.aspx
 - www.atg.wa.gov/credit-freeze-fraud-alerts



**STATE OF WASHINGTON
HEALTH CARE AUTHORITY**

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>

Parent or Guardian of <<Name1>>

<<Name2>>

<<Address1>>

<<Address2>>

<<City>><<State>><<Zip>>

<<Date>>

To the Parent or Guardian of <<Name 1>>:

SUBJECT: Notification Regarding Your Minor's Protected Health Information

The Washington State Health Care Authority (HCA) is sending this letter to you to make sure you are made aware of an incident resulting in the unauthorized disclosure of some of your minor's Apple Health (Medicaid) information by an individual employee of HCA. We have learned that the following kinds of information were disclosed—some or all of which may apply to your minor:

- Name
- Address and phone number
- Social Security number
- Date of birth
- Apple Health ID
- Medical procedure information
- Medical diagnosis information

Although we have no evidence that the Apple Health information was inappropriately used, we need to inform you of this incident in writing. We also want to describe the steps we are taking to respond to this incident and outline the additional steps you can take to protect your minor from any potential harm.

Description of Incident

Between November 15, 2013, and December 24, 2015, an HCA employee emailed spreadsheets containing Apple Health client information to another state employee who should not have received the information. While both the HCA employee and the recipient of the emails assert that the information was shared only for work purposes and was not used inappropriately in any manner, we cannot be sure that this is the case. HCA became aware of the potential unauthorized disclosure of some of your minor's Apple Health information on about December 16, 2015, and the agency began taking immediate steps to assess and investigate the matter.

What We Have Done in Response to the Incident

Upon discovery of this incident, HCA promptly took a number of steps including:

- Investigating how the information was transferred and used.
- Taking possession of all information that was sent by the HCA employee and received by the other state employee.
- Conducting separate interviews with both employees to understand the circumstances surrounding the exchange of information and to determine what they did with the information. Both employees assert that the exchange of information occurred because the HCA employee needed technical assistance with spreadsheets, and that the information was not used for any additional unauthorized purposes or forwarded to any other unauthorized recipients.
- Terminating the employment of the HCA staff involved in the incident.

- Reminding all HCA employees as to the importance of protecting private health and personal information.
- Planning additional training for our staff to address this specific issue.
- Notifying the appropriate federal officials for further investigation and potential criminal review.

What We Are Doing to Protect Your Minor's Information

To help you detect the possible misuse of your minor's information, we are providing you, the parent or guardian, with a complimentary one-year membership in Family Secure® from Experian®. Family Secure monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if the minor has a credit report, a potential sign that his or her identity has been stolen.

To receive the complimentary Family Secure product, you, as the parent or guardian, must enroll at the web site with your activation code listed below. This activation code can only be used by the parent or guardian of the minor. Please keep in mind that once activated, the code cannot be re-used for another enrollment.

Activate Family Secure Now in Three Easy Steps

1. ENSURE that you enroll by: May 12, 2016 (Your code will not work after this date.)
2. VISIT the Family Secure Web Site to enroll: <http://www.familysecure.com/enroll>
3. PROVIDE your activation code: <<Code>>

If you have questions or need an alternative to enrolling online, please call 1-877-288-8057 and provide engagement number: **PC99053**.

Once your enrollment in Family Secure is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-288-8057.

HCA has also set up an **Incident Response Line** to address any questions you may have about this Notice or the incident. Please contact the **Incident Response Line** at: 1-877-866-9702.

What You Can Do to Protect Your Minor's Information

There are additional actions you can consider taking to reduce the chances of identity theft or fraud. Please refer to the final page of this Notice for additional information.

HCA takes our role of safeguarding your minor's personal information and using it in an appropriate manner very seriously. We are committed to protecting the confidentiality of our clients' information and apologize for the concern this incident may have caused. We assure you that we are doing everything we can to prevent future incidents.

Additional Actions to Help Reduce your Chances of Identity Theft or Fraud

Place a 90-day Fraud Alert on your Credit File

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
1-800-525-6285
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

Place a Security Freeze on your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

Order your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

Obtain more Information about Identity Theft and ways to Protect Yourself

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.
- The Washington State Attorney General's Office has information at:
 - www.atg.wa.gov/guardit.aspx
 - www.atg.wa.gov/credit-freeze-fraud-alerts



**STATE OF WASHINGTON
HEALTH CARE AUTHORITY**

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
The Estate of <<Name1>>
<<Address1>>
<<Address2>>
<<City>> <<State>> <<Zip>>

<<Date>>

To the Estate of <<Name 1>>:

SUBJECT: Notification to the Estate of the Deceased Regarding Deceased's Protected Health Information

The Washington State Health Care Authority (HCA) is sending this letter to you to make sure you are made aware of an incident resulting in the unauthorized disclosure of some of the deceased's Apple Health (Medicaid) information by an individual employee of HCA. We have learned that the following kinds of information were disclosed—some or all of which may apply to the deceased:

- Name
- Address and phone number
- Social Security number
- Date of birth
- Apple Health ID
- Medical procedure information
- Medical diagnosis information

Although we have no evidence that the Apple Health information was inappropriately used, we need to inform you of this incident in writing. We also want to describe the steps we are taking to respond to this incident and outline the additional steps you can take.

Description of Incident

Between November 15, 2013, and December 24, 2015, an HCA employee emailed spreadsheets containing Apple Health client information to another state employee who should not have received the information. While both the HCA employee and the recipient of the emails assert that the information was shared only for work purposes and was not used inappropriately in any manner, we cannot be sure that this is the case. HCA became aware of the potential unauthorized disclosure of some of the deceased's Apple Health information on about December 16, 2015, and the agency began taking immediate steps to assess and investigate the matter.

What We Have Done in Response to the Incident

Upon discovery of this incident, HCA promptly took a number of steps, including:

- Investigating how the information was transferred and used.
- Taking possession of all information that was sent by the HCA employee and received by the other state employee.
- Conducting separate interviews with both employees to understand the circumstances surrounding the exchange of information and to determine what they did with the information. Both employees assert that the exchange of information occurred because the HCA employee needed technical assistance with spreadsheets and that the information was not used for any additional unauthorized purposes or forwarded to any other unauthorized recipients.
- Terminating the employment of the HCA staff involved in the incident.

- Reminding all HCA employees as to the importance of protecting private health and personal information.
- Planning additional training for our staff to address this specific issue.
- Notifying the appropriate federal officials for further investigation and potential criminal review.

HCA has also set up an **Incident Response Line** to address any questions you may have about this Notice or the incident. Please contact the **Incident Response Line** at: 1-877-866-9702.

What You Can Do to Protect the Deceased's Information

There are additional actions you can consider taking to reduce the chances of theft of the deceased's identity or fraud. Please refer to the final page of this Notice for additional information.

HCA takes our role of safeguarding the deceased's personal information and using it in an appropriate manner very seriously. We are committed to protecting the confidentiality of our clients' information and apologize for the concern this incident may have caused. We assure you that we are doing everything we can to prevent future incidents.

Additional Actions to Help Reduce your Chances of Identity Theft or Fraud

Place a 90-day Fraud Alert on your Credit File

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax

1-800-525-6285

www.equifax.com

Experian

1-888-397-3742

www.experian.com

TransUnion

1-800-680-7289

www.transunion.com

Place a Security Freeze on your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

Order your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Use Tools from Credit Providers

Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

Obtain more Information about Identity Theft and ways to Protect Yourself

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.
- The Washington State Attorney General's Office has information at:
 - www.atg.wa.gov/guardit.aspx
 - www.atg.wa.gov/credit-freeze-fraud-alerts