

BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

Lynn Sessions
direct dial: 713.646.1352
lsessions@bakerlaw.com

December 14, 2015

VIA EMAIL (securitybreach@atg.wa.gov)

Bob Ferguson
Attorney General of Washington
Consumer Protection Division
800 Fifth Avenue, Suite 2000
MS TB 14
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

On behalf of our client, PeaceHealth, we submit this supplemental notice regarding a data security incident that involved potential access to patient information by a former employee of PeaceHealth. As reported to your office on November 30, 2015, PeaceHealth first learned on October 9 that an employee who no longer works at PeaceHealth accessed patient information in separate instances from a home computer using third-party websites, including insurance verification websites and prior authorization portals beginning on June 15, 2015. We immediately began working to remove access which was accomplished on October 12, 2015. PeaceHealth reported the unauthorized access to law enforcement and immediately began an investigation. Law enforcement advised us on December 3, 2015, that additional persons were potentially affected by this incident and that the information the former employee accessed included patients' names, dates of birth, addresses, telephone numbers, gender, insurance information, and in some instances diagnoses, medications and social security numbers.

PeaceHealth engaged the website and portal companies as well as law enforcement in its investigation but there is no indication that the former employee accessed the information for identity theft purposes. PeaceHealth has established a dedicated call center to assist patients with any questions they may have. To help prevent this from happening in the future, PeaceHealth has received assurances from

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

Attorney General of Washington

December 14, 2015

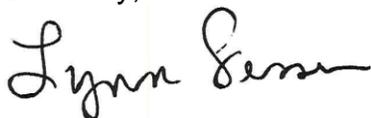
Page 2

the website and portal companies that the former employee no longer has access to their systems. PeaceHealth is also enhancing the processes that will ensure removal of access to third-party companies when an employee leaves PeaceHealth.

PeaceHealth timely notified an additional 812 Washington residents in substantially the same form as the letters attached hereto on today, December 14, 2015.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "Lynn Sessions". The signature is written in a cursive style with a large initial "L" and a long, sweeping underline.

Lynn Sessions

Enclosures



PeaceHealth

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

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

<<Date>>

Dear <<Name1>>:

PeaceHealth is committed to maintaining the privacy and security of our patients' information. Regrettably, we are writing to inform you of an incident involving some of that information.

On October 9, 2015, we first learned that an employee who no longer works at PeaceHealth accessed patient information from a home computer using third-party websites, including insurance verification websites and prior authorization portals from June 15, 2015 to October 12, 2015. We reported the unauthorized access to law enforcement and immediately began an investigation. Law enforcement advised us on December 3, 2015, that your information was included in the former employee's access and may have included your name, date of birth, age, address, phone, gender, language and insurance information. Your social security number was not included.

Even though we have no evidence that your information has been used inappropriately, we wanted to notify you of this incident and assure that we take it very seriously. We recommend that you regularly review the explanation of benefits that you receive for your health insurer. If you see services that you did not receive, immediately contact your insurer.

PeaceHealth sincerely apologizes for this incident and any concern this may cause you. Your privacy is a very high priority to us. The website and portal companies have ensured PeaceHealth that the user no longer has access to their systems. To help prevent future incidents such as this, we are enhancing the processes that will ensure removal of access to third-party companies when an employee leaves PeaceHealth. In the course of the investigation of this incident, the former employee's personal computer and other electronic information devices were obtained and reviewed, which should ensure that all PeaceHealth patient information has been secured.

Should you have any questions or concerns, please call 1-877-879-5081, Monday through Friday between 6:00 a.m. and 6:00 p.m. Pacific Time.

Sincerely,

Gary T. Chiodo, DMD, FACD
Vice President, Organizational Integrity



PeaceHealth

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

<<mail id>>
Parent or Guardian of
<<Name1>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear Parent or Guardian of <<Name1>>:

PeaceHealth is committed to maintaining the privacy and security of our patients' information. Regrettably, we are writing to inform you of an incident involving some of that information regarding your minor child.

On October 9, 2015, we first learned that an employee who no longer works at PeaceHealth accessed patient information from a home computer using third-party websites, including insurance verification websites and prior authorization portals from June 15, 2015 to October 12, 2015. We reported the unauthorized access to law enforcement and immediately began an investigation. Law enforcement advised us on December 3, 2015, that your information was included in the former employee's access and may have included your child's name, date of birth, child's age, address, phone, gender, language and insurance information. Your child's social security number was not included.

Even though we have no evidence that your child's information has been used inappropriately, we wanted to notify you of this incident and assure that we take it very seriously. We recommend that you regularly review the explanation of benefits that you receive for your child's health insurer. If you see services that your child did not receive, immediately contact the insurer.

PeaceHealth sincerely apologizes for this incident and any concern this may cause you. Your privacy and your child's privacy are a very high priority to us. The website and portal companies have ensured PeaceHealth that the user no longer has access to their systems. To help prevent future incidents such as this, we are enhancing the processes that will ensure removal of access to third-party companies when an employee leaves PeaceHealth. In the course of the investigation of this incident, the former employee's personal computer and other electronic information devices were obtained and reviewed, which should ensure that all PeaceHealth patient information has been secured.

Should you have any questions or concerns, please call 1-877-879-5081, Monday through Friday between 6:00 a.m. and 6:00 p.m. Pacific Time.

Sincerely,

Gary T. Chiodo, DMD, FACD
Vice President, Organizational Integrity



PeaceHealth

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

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

<<Date>>

Dear <<Name1>>:

PeaceHealth is committed to maintaining the privacy and security of our patients' information. Regrettably, we are writing to inform you of an incident involving some of that information.

On October 9, 2015, we first learned that an employee who no longer works at PeaceHealth accessed patient information from a home computer using third-party websites, including insurance verification websites and prior authorization portals from June 15, 2015 to October 12, 2015. We reported the unauthorized access to law enforcement and immediately began an investigation. Law enforcement advised us on December 3, 2015, that your information was included in the former employee's access and may have included your name, date of birth, age, address, phone, gender, language and Medicare information, which contains your social security number.

Even though we have no evidence that your information has been used inappropriately, we wanted to notify you of this incident and assure that we take it very seriously. In an abundance of caution, we are offering you a free one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.** We also recommend that you regularly review the explanation of benefits that you receive for your health insurer. If you see services that you did not receive, immediately contact your insurer.

PeaceHealth sincerely apologizes for this incident and any concern this may cause you. Your privacy is a very high priority to us. The website and portal companies have ensured PeaceHealth that the user no longer has access to their systems. To help prevent future incidents such as this, we are enhancing the processes that will ensure removal of access to third-party companies when an employee leaves PeaceHealth. In the course of the investigation of this incident, the former employee's personal computer and other electronic information devices were obtained and reviewed, and all PeaceHealth patient information has been deleted.

Should you have any questions or concerns, please call 1-877-879-5081, Monday through Friday between 6:00 a.m. and 6:00 p.m. Pacific Time.

Sincerely,

Gary T. Chiodo, DMD, FACD
Vice President, Organizational Integrity

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **March 19, 2016** (You will not be able to enroll after this date.)
2. VISIT the ProtectMyID Web Site: www.protectmyid.com/redeem
3. PROVIDE Your Activation Code: <<Code>>

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **PC98104**.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - Daily Bureau Credit Monitoring: Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

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 877-288-8057.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.