

RECEIVED

AUG 05 2019

BakerHostetler

CONSUMER PROTECTION

Baker & Hostetler LLP

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
www.bakerlaw.com

August 2, 2019

Lynn Sessions  
direct dial: 713.646.1352  
lsessions@bakerlaw.com

**VIA OVERNIGHT MAIL**

Attorney General Joseph Foster  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: *Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, Presbyterian Healthcare Services ("Presbyterian") regarding an unauthorized person who may have accessed some employee email accounts.

On June 6, 2019, Presbyterian discovered anonymous, unauthorized access gained through a deceptive email to some of Presbyterian's workforce around May 9, 2019. The email accounts included some Presbyterian patient and members' names, social security numbers, dates of birth, clinical information and/or health insurance information. Presbyterian is continuing to investigate and conduct a thorough review of each impacted Presbyterian email account and may mail additional notification letters in the coming week.

Presbyterian mailed letters in substantially the same form as the attached to four New Hampshire residents beginning on August 2, 2019, pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR §§ 160.103 and 164.400 *et seq.* For those individuals whose social security number was contained within the email accounts, Presbyterian is offering complimentary credit monitoring and identity protection services. To help prevent something like this from happening again, Presbyterian is taking several steps and implementing additional security measures to further protect its email environment. In addition, all workforce members annually must successfully complete mandatory training about the importance and requirement to safeguard all information. In particular, workforce members have received and will continue to receive reminders about safeguarding information stored electronically and how to avoid phishing scams.

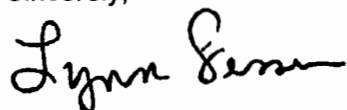
As a covered entity under HIPAA, Presbyterian maintains procedures for responding to incidents such as this, and notification to the New Hampshire residents is provided in accordance with those

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

procedures. Notification to the Attorney General is being provided in compliance with NH Rev. State § 359-C:20 (2015).<sup>1</sup>

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, flowing style.

Lynn Sessions

Enclosure

---

<sup>1</sup> This report is not and does not constitute a waiver of Presbyterian's objection that the State of New Hampshire lacks personal jurisdiction over Presbyterian regarding any claims related to this incident.



C/O ID Experts  
 PO Box 4219  
 Everett WA 98204

ENDORSE



VER FIRST NAME LAST NAME

ADDRESS1

ADDRESS2

CSZ

BREAK

SEQ  
 CODE 2D COUNTRY

To Enroll, Please Call:

(833) 297-6405

Or Visit:

<https://ide.myidcare.com/presbyterian-protect>

Enrollment Code: <<XXXXXXXXXX>>

August 2, 2019

Dear <<First Name>> <<Last Name>>,

At Presbyterian, we are committed to protecting the privacy of our patients and members. You are receiving this letter because you have received health care services through a Presbyterian provider and/or you have been a Presbyterian Health Plan member.

Recently, Presbyterian discovered that an unauthorized person may have accessed some employee email accounts that contained health information. As part of our commitment to you, we want to explain what occurred, share steps we are taking to prevent this from happening again and offer resources for you.

On June 6, 2019, Presbyterian discovered anonymous, unauthorized access gained through a deceptive email to some of Presbyterian’s workforce members around May 9, 2019. We believe that the unauthorized access to these email accounts was part of a scam or deceptive email trying to get information, known as “phishing.” These email accounts included your name and social security number and might have contained your date of birth, clinical and/or health insurance information.

We are very sorry that unauthorized access to some of the workforce members’ emails occurred. We are not aware of any improper use, or attempted use of your information, but we believe it is important to notify you of this incident.

We are continuing to investigate and conduct a thorough review of each impacted Presbyterian email account. Once we became aware of this incident, Presbyterian secured these email accounts and alerted federal law enforcement.

We take the responsibility of safeguarding your information very seriously. To help prevent this incident from happening again, Presbyterian is taking several steps and implementing additional security measures to further protect our email system. In addition, all workforce members annually must successfully complete mandatory training about the importance and requirement to safeguard all information. In particular, workforce members have received, and will continue to receive, reminders about safeguarding information stored electronically and how to avoid phishing scams.

We recommend that you review the statements that you receive from your health plan or your health care providers regarding your health care services. If you see any service that you believe you did not receive, please contact the health plan or provider immediately.

In addition, at no cost to you, we are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We want to assure you that Presbyterian is committed to protecting the privacy and confidentiality of every individual’s information.

If you have any questions, please call (833) 297-6405 or go to <https://ide.myidcare.com/presbyterian-protect> for assistance or for any additional questions you may have, Monday through Friday, 7:00 a.m. to 7:00 p.m. Mountain Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Sophia Collaros", written in a cursive style.

Sophia Collaros  
Privacy Officer

2 de agosto del 2019

Estimado(a) <<First Name>> <<Last Name>>,

Aquí en Presbyterian, nos comprometemos a proteger la privacidad de nuestros pacientes y asegurados. Le enviamos la presente porque usted ha recibido servicios de un proveedor de atención médica de Presbyterian y/o ha sido asegurado de Presbyterian Health Plan.

Recientemente, Presbyterian descubrió que a lo mejor una persona no autorizada obtuvo acceso a las cuentas de correo electrónico de unos empleados, las cuales contenían datos de salud. Como parte de nuestro compromiso con usted, queremos explicarle lo sucedido, contarle las medidas que estamos llevando a cabo para que no vuelva a suceder y ofrecerle unos recursos.

El 6 de junio del 2019, Presbyterian descubrió que hubo acceso anónimo no autorizado que se obtuvo mediante un mensaje engañoso enviado por correo electrónico a algunos de los empleados de Presbyterian alrededor del 9 de mayo del 2019. Creemos que el acceso no autorizado a esas cuentas de correo electrónico forma parte de una estafa o un fraude con la intención de obtener información por correo electrónico, que en inglés se llama “*phishing*” [fraude electrónico]. Dichas cuentas de correo electrónico incluían su nombre y número de seguro social y a lo mejor también tenían su fecha de nacimiento, datos clínicos y/o de seguro médico.

Sentimos mucho que haya sucedido el acceso no autorizado a las cuentas de correo electrónico de algunos de los empleados. No sabemos que su información se haya utilizado inapropiadamente, o que se haya intentado hacerlo, sin embargo creemos que es importante avisarle de este incidente.

Seguimos investigando y llevando a cabo una revisión completa de cada cuenta de correo electrónico afectada de Presbyterian. Una vez que nos dimos cuenta de este incidente, Presbyterian protegió dichas cuentas de correo electrónico y avisó a los cuerpos policiales federales.

Tomamos muy en serio la responsabilidad de salvaguardar su información. Para ayudar a prevenir que suceda de nuevo este incidente, Presbyterian está realizando varios remedios e implementando medidas de seguridad adicionales a fin de proteger más a fondo nuestro sistema de correo electrónico. Además cada año, todos los empleados tienen que realizar con éxito una capacitación obligatoria sobre la importancia y obligación de salvaguardar toda la información. En particular, los empleados han recibido y seguirán recibiendo notas para recordarles que deben salvaguardar la información que se guarda electrónicamente y cómo evitar las estafas de fraudes electrónicos.

Recomendamos que revise todos los estados de cuenta que reciba de su plan de seguro médico o de sus proveedores de atención médica con respecto a los servicios médicos. Si se indica un servicio que usted cree que no ha recibido, favor de comunicarse enseguida con el plan de seguro médico o el proveedor de atención médica.

Además, sin costarle nada a usted, le estamos ofreciendo servicios de protección contra el robo de identidad mediante ID Experts® para proporcionarle MyIDCare™. Los servicios que ofrece MyIDCare incluyen: 12 meses de monitorización de su crédito y CyberScan, una póliza de seguro de reembolso de \$1.000.000 y servicios plenamente dirigidos de recuperación contra el robo de identidad. Con esta protección, MyIDCare le ayudará a resolver problemas si su identidad se ha puesto en riesgo.

Queremos asegurarle de que Presbyterian se compromete a proteger la privacidad y confidencialidad de los datos de todas las personas.

Si usted tiene preguntas, favor de llamar al (833) 297-6405 o vaya a <https://ide.myidcare.com/presbyterian-protect> para recibir ayuda o para conseguir respuestas a las preguntas que tenga, de lunes a viernes, de las 7:00 de la mañana a las 7:00 de la tarde, tiempo de la zona de montaña.

Atentamente,

A handwritten signature in black ink, appearing to read "Sophia Collaros", enclosed in a large, stylized circular flourish.

Sophia Collaros  
Encargada de privacidad



9585230303

### Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/presbyterian-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 MyIDCare 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, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at (833) 297-6405 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](http://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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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 (<http://www.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](http://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](http://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/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_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.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://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/](http://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](http://www.riag.ri.gov), Telephone: 401-274-4400

**Connecticut Attorney General's Office,** 55 Elm Street, Hartford, CT 06106, [www.ct.gov/ag](http://www.ct.gov/ag) Telephone:1-860-808-5318

**Office of the Massachusetts Attorney General,** One Ashburton Place, Boston, MA 02108  
[www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html), Telephone 1-617-727-8400

**North Carolina Attorney General's Office,** 9001 Mail Service Centre, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400 / 1-877-566-7226,

- *Rhode Island Attorney General's Office,* 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

**If you are a resident of Massachusetts or Rhode Island,** note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

**If you are a resident of West Virginia,** you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

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