

RECEIVED

SEP 16 2019

CONSUMER PROTECTION

BakerHostetler

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

September 13, 2019

VIA OVERNIGHT MAIL

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

Re: *Notice of Incident*

Dear Attorney General Foster:

I am writing on behalf of our client, Community Healthlink (“CHL”), to notify you of a security incident involving three New Hampshire residents.¹ CHL is a health care provider and a covered entity under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”).

On July 16, 2019, as a result of an ongoing investigation, CHL determined that information belonging to patients and current/former employees was potentially affected by an email security incident. The investigation began on April 18, 2019 when CHL learned that an unauthorized individual gained access to two CHL employees’ email accounts. The access was for a limited time on April 18th. CHL immediately secured the accounts and a leading computer forensic firm was engaged to assist the investigation. The investigation was unable to determine whether the unauthorized person actually viewed any emails in the accounts.

On June 17, 2019, CHL notified 4,015 individuals in accordance with HIPAA while it continued its investigation into the contents of the email accounts. As a result of this ongoing review CHL determined that the accounts contained one or more of the following data elements

¹ This report does not waive CHL’s objection that New Hampshire lacks personal jurisdiction over CHL related to this incident

September 13, 2019

Page 2

for three New Hampshire residents: name, date of birth, Social Security number and/or driver's license number, and Protected Health Information (as defined by HIPAA).

On September 13, 2019, CHL will mail notification letters to the three New Hampshire residents whose Personal Information, as defined by N.H. Rev. Stat. § 359-C:19 IV(a), was found in the accounts.² The letters are being mailed via United States First-Class mail, in substantially the same form as the enclosed letter versions.

CHL is offering eligible New Hampshire residents a complimentary one-year membership in credit monitoring and identity theft protection services through Experian. Residents are eligible if their name and Social Security number and/or driver's license number were involved. Eligible individuals may enroll in the credit monitoring services online or via phone until November 17, 2019, instructions for which are provided in the notification letter. The notification letter provides a toll-free number to call with questions about the credit monitoring services. CHL is also providing a separate telephone number for individuals to call with any questions about the incident.

To help prevent a similar incident from occurring in the future CHL is re-educating employees regarding phishing emails and enhancing its existing security measures.

CHL takes the security of personal information very seriously and is committed to protecting personal information. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Eric A. Packel
Partner

Enclosures

² An additional 26 CHL patients, who are also New Hampshire residents, are being notified in accordance with HIPAA only. CHL previously notified eight New Hampshire residents in accordance with HIPAA as part of the June 17, 2019 notifications. CHL is now notifying your office specifically of the three New Hampshire residents whose Social Security numbers and/or driver's license numbers were found in the email accounts, because N.H. Rev. Stat. § 359-C:19 IV(a) specifically includes Social Security numbers and driver's license numbers in the definition of personal information.

UMass Memorial Community Healthlink
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



September 6, 2019

[REDACTED]
[REDACTED]
[REDACTED]

C-1

Dear [REDACTED]:

Community Healthlink (“CHL”), a member of the UMass Memorial Health Care System, takes the privacy and security of its patients’ information very seriously. Regrettably, we write to inform you of an incident involving some of your information. This notice describes the incident, outlines the measures we have taken in response, and steps you can take.

On July 16, 2019, as a result of our ongoing investigation, we determined that some of your information was potentially affected by an email security incident. Our investigation began on April 18, 2019 when we learned that an unauthorized individual gained access to two CHL employees’ email accounts. The access was for a limited time on April 18th. We immediately secured the accounts and a leading computer forensic firm was engaged to assist our investigation. The investigation was unable to determine whether the unauthorized person actually viewed any emails in the accounts.

We conducted a comprehensive review of the emails and attachments in the accounts to identify information that was potentially accessible to the unauthorized person. As a result of this review, on July 16, 2019, we determined that the accounts contained some of your information, which may have included your name, date of birth, Social Security number, client identification number, and limited treatment and/or clinical information, such as provider name, date of service, medications, and/or facility name.

Although we have no evidence that any of your information was actually accessed or that it has been misused, in an abundance of caution, we are offering you a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, 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 review statements you receive from your healthcare provider. If you see services you did not receive, please contact your provider immediately.

We regret any concern or inconvenience this incident may cause you. To help prevent something like this from happening in the future, CHL continues to assess its systems and implement safeguards to address risks. We are also reinforcing employee training on how to detect and avoid phishing emails. If you have any questions, please call 1-877-420-0507, Monday through Friday, between 8:00 a.m. and 5:00 p.m. Eastern Time.

Sincerely,

A handwritten signature in black ink that reads "Nicole Gagne".

Nicole Gagne
President and CEO

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **November 17, 2019** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code:** XXXXXXXXXX

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **DB14264** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

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 on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

UMass Memorial Community Healthlink
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



September 6, 2019

[Redacted]

J-4

Dear [Redacted]

Community Healthlink (“CHL”), a member of the UMass Memorial Health Care System, takes the privacy and security of our former and current employees’ and candidates’ information very seriously. Regrettably, we write to inform you of an incident involving some of your information. This notice describes the incident, outlines the measures we have taken in response, and steps you can take.

On July 16, 2019, as a result of our ongoing investigation, we determined that some of your information was potentially affected by an email security incident. Our investigation began on April 18, 2019 when we learned that an unauthorized individual gained access to two CHL employees’ email accounts. The access was for a limited time on April 18th. We immediately secured the accounts and a leading computer forensic firm was engaged to assist our investigation. The investigation was unable to determine whether the unauthorized person actually viewed any emails in the accounts.

We conducted a comprehensive review of the emails and attachments in the accounts information that was potentially accessible to the unauthorized person. As a result of this review, on July 16, 2019, we determined that the accounts contained some of your information, which may have included your name, date of birth, and driver’s license number.

Although we have no evidence that any of your information was actually accessed or that it has been misused, in an abundance of caution, we are offering you a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

We regret any concern or inconvenience this incident may cause you. To help prevent something like this from happening in the future, CHL continues to assess its systems and implement safeguards to address risks. We are also reinforcing employee training on how to detect and avoid phishing emails. If you have any questions, please call 1-877-420-0507, Monday through Friday, between 8:00 a.m. and 5:00 p.m. Eastern Time.

Sincerely,

A handwritten signature in cursive script that reads 'Nicole Gagne'.

Nicole Gagne
President and CEO

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **November 17, 2019** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: XXXXXXXXXX

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **DB14264** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

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 on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, 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.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.