MAYNARD
COOPER GALE

Adam Griffin
DIRECT 205.415.4903
EMAIL agriffin@maynardcooper.com

April 1, 2022

Attorney General Gordon McDonald
Office of Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of a Security Incident

Dear Attorney General McDonald,

I am writing to let you know that our client, Summit BHC West Virginia, LLC d/b/a Highland Hospital ("Highland"), experienced a security incident that affected the personally identifiable information ("PII") of some patients and former employees, including one (1) individual in New Hampshire. We are providing notice to your office pursuant to N.H. Rev. Stat. § 359-C:19, *et seq.* This matter has also been reported to the U.S. Department of Health and Human Services pursuant to 45 CFR §164.408.

On October 26, 2021 an unauthorized party gained access to the ADP portal for one employee, and altered the user's payroll information. This activity kicked off an alert that was investigated by Highland IT with the help of outside experts. The investigation revealed that an unauthorized third party successfully logged in to five (5) employee e-mail accounts for varying periods of time. A comprehensive review of these accounts resulted in the identification of personal information belonging to Highland patients and employees. These individuals were notified March 31, 2022. A copy of the notice is enclosed as Exhibit A, which included an offer of complimentary credit monitoring and identity protection services through Experian.

We cannot tell from the forensic evidence if any of the files containing personal information were actually viewed by the unauthorized party. The unauthorized actions we are able to see in these email accounts all appear to be in furtherance of unsuccessful payment fraud attempts. Efforts to change employee pay details were not successful. There have been no reports of any actual or attempted misuse of personal information as a result of this incident.

After discovering this event, Highland took steps to terminate the unauthorized party's access to the O365 System. This included, for example, resetting the passwords for the compromised user accounts, and implementing multi-factor authentication for *all* user e-mail accounts. Highland has implemented new threat monitoring and prevention tools to further secure the Highland network against cyber threats and will be introducing additional authentication and security training requirements for all of its employees in 2022 to counteract phishing and other social engineering techniques. Highland has also expanded corporate IT staff to increase the ability to manage the environment more securely.

Please do not hesitate to let me know if you have any questions or would like additional information.

Sincerely,

Adam Griffin

Enclosure

Highland Hospital
HIGHLAND CAN HELP

Return Mail Processing
PO Box 999
Suwanee, GA 30024

26 2 5849 **********AUTO**5-DIGIT 25064
SAMPLE A. SAMPLE - LVA
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

March 31, 2022

Dear Sample A. Sample:

I hope this letter finds you well. I am writing to let you know about an e-mail security incident at Highland Hospital that may have involved the personal information we have on file for you. We have no indications that any personal information has been misused as a result of this incident. However, we take patient privacy very seriously, and want to make sure that you are aware of what happened so that you can take the appropriate precautions you feel are needed to protect your identity. We have enclosed information on several identity protection resources.

What Happened?

On October 26, 2021 an unauthorized party gained access to the ADP portal for one of our employees, and altered the user's payroll information. This activity kicked off an alert that was investigated by Highland IT with the help of outside experts. The investigation revealed that an unauthorized third party successfully logged in to some of our employee e-mail accounts. The unauthorized actions we identified within the accounts were all focused on attempts to perpetrate a payment fraud. All of these attempts were blocked. Our experts performed a comprehensive review of these accounts, and determined that one or more of these accounts contained files that included information about you. We cannot tell from available forensic evidence whether any e-mails were actually viewed by the unauthorized party, but it is possible. We have no reason to believe your personal information has been misused.

What Information Was Available?

Files available within the affected e-mail accounts may have included: (1) patient contact information (such as patient name, guarantor name, address, email address); (2) Social Security Number; (3) date of birth; (4) health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber number); (5) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (6) billing, payment, and claims information (invoices, payment details, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all of these data fields may have been involved for all individuals.

What We Are Doing

We are committed to protecting the information we maintain. We have taken steps to further secure our e-mail environment, and will continue to focus on strengthening the cyber-resiliency of our company. This has included, for example, resetting users' passwords, adding multi-factor authentication, and implementing new threat monitoring and prevention tools to further secure the Highland network against cyber threats.

What You Can Do

The enclosed Identity Protection Reference Guide includes information on general steps you can take to monitor and protect your personal information. We would encourage you to review these materials, and take the appropriate steps you feel are warranted. We are also offering one year of complimentary credit monitoring and identity protection services. If you would like to enroll in this service, please review the enclosed instructions.

We are sorry for any inconvenience this may cause. If you have any questions, please reach out to our dedicated team at (888) 829-6550, Monday through Friday from 8 am – 10 pm Central, or Saturday or Sunday from 10 am – 7 pm Central (excluding major U.S. holidays).

Sincerely,

Nadine Dexter
Chief Executive Officer

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. 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. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is only necessary to contact <u>one</u> of these bureaus and use only <u>one</u> 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 should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact <u>each</u> of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can obtain additional information about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the FTC. You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

****

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

We are offering you a one-year, complimentary membership for IdentityWorks℠, a product offered by Experian®, to help with detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: June 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

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 at (888) 829-6550 by June 30, 2022. The call center is open Monday through Friday 8 am - 10 pm CST, Saturday and Sunday 10 am - 7 pm CST (excluding major U.S. holidays). Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the identity restoration services by Experian.

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 829-6550. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.