1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

April 21, 2023

Via Online Reporting
Office of the Maine Attorney General
Consumer Protection Division
6 State House Station
Augusta, ME 04333

RE: Notice of Data Event

Dear Sir or Madam:

We represent Robeson Health Care Corporation ("RHCC"), a 501(c)(3) nonprofit network of health centers serving Pembroke, North Carolina and its surrounding communities. This submission is provided pursuant to the Maine Notice of Risk to Personal Data Act, M.E. STAT. ANN. T. 10 § 1346, *et seq*, which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maine.

On February 21, 2023, RHCC became aware that its computer network was affected by malware. RHCC disconnected its network from the internet and partnered with computer forensic specialists to restore its systems safely and understand the nature and scope of the event. RHCC commenced a thorough investigation which determined an unauthorized third-party gained access to its systems between February 17 and February 21, 2023. RHCC has no indication that its electronic medical records (EMR) data bases were accessed without authorization. However, based on available evidence, RHCC concluded on March 31, 2023, that sensitive personal information could have been viewed or taken during the period of unauthorized access. The information potentially accessible on the network could have included patient name, address, Social Security number, date of birth, treatment information/diagnosis, treating physician, medical record number (MRN), patient ID number, Medicare/Medicaid number, prescription information, health insurance information, and treatment costs.

On or about April 21, 2023, RHCC began providing, via U.S. regular mail, notice of the incident to the potentially affected individuals. A sample copy of the notice is attached as Exhibit "A" for your records. RHCC provided this notification to one (1) Maine resident. RHCC also posted substitute notification of the data event on its website homepage beginning on April 21, 2023, while the investigation to confirm the full impacted population is still ongoing.

RHCC is providing written notice of this event to the affected individuals that includes a brief description of the incident, encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements, credit reports and explanation of benefits (EOBs), report any suspicious activity to the financial institution or the appropriate service provider, and to file a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. RHCC also enclosed documentation containing contact information for the major consumer reporting bureaus, state-specific regulators, a dedicated call center, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so. RHCC is also offering identity theft monitoring and restoration services through Experian to impacted adults and minors for whom RHCC has address information for. The services include single bureau daily credit reporting, continuous identity monitoring, account activity alerts, and $1 million identity theft insurance with no deductible.

In response to the suspicious activity, RHCC disconnected it network from the internet and partnered with computer forensics specialists to restore its systems safely. RHCC conducted a thorough investigation to understand the nature and scope of the event. RHCC reset passwords and enabled multi-factor authentication for all users. RHCC continues to review the policies and procedures in place prior to the event, to identify ways to strengthen its security going forward. RHCC has also notified other state and federal regulators as required.

I believe this provides you with all information necessary for your purposes and to comply with Maine law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit A

RHCC
Your Health Care Guardian

Return Mail Processing
PO Box 999
Suwanee, GA 30024

45 1 15039 **********AUTO**5-DIGIT 28348
SAMPLE A. SAMPLE - Patient
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

April 21, 2023

RE: NOTICE OF DATA SECURITY EVENT

Dear Sample A. Sample:

At Robeson Health Care Corporation ("RHCC"), we take the privacy and security of patient information seriously. We are therefore notifying you of a data security event. Please read this letter carefully.

What Happened?
On February 21, 2023, RHCC became aware that our computer network was affected by malware. We disconnected our network from the internet and partnered with computer forensic specialists to restore our systems safely and understand the nature and scope of the event. We commenced a thorough investigation which determined an unauthorized third-party gained access to our systems between February 17 and February 21, 2023. RHCC has no indication that our electronic medical records (EMR) data bases were accessed without authorization. However, based on available evidence, we concluded on March 31, 2023, that your sensitive personal information could have been viewed or taken during the period of unauthorized access. We are notifying you accordingly, and out of an abundance of caution.

What Information Was Involved?
The information potentially accessible on our network could have included your name, address, Social Security number, date of birth, treatment information/diagnosis, treating physician, medical record number (MRN), patient ID number, Medicare/Medicaid number, prescription information, health insurance information, and treatment costs. **We stress that to date, we have received no reports or evidence to suggest fraud or identity theft occurred as a result of this event.**

What We Are Doing
Upon discovery of the suspicious activity, we disconnected our network from the internet and partnered with computer forensics specialists to restore our systems safely. We conducted a thorough investigation to understand the nature and scope of the event. We reset passwords and enabled multi-factor authentication for all users. We continue to review the policies and procedures in place prior to the event, to identify ways to strengthen our security going forward.

As an added precaution to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for twelve (12) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident. This assistance may include, 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 Identity Restoration is available to you for 12 months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by July 31, 2023** (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 that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-796-8636 by **July 31, 2023**. Please be prepared to provide engagement number B090293 as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

We encourage you remain vigilant for instances of fraud or identity theft, from any source. You should monitor your account statements, credit reports, and explanations of benefits (EOBs) and report any suspicious activity to your financial institution or the appropriate service provider. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation titled "Additional Steps to Help Protect Your Information" for more information and recommended steps you can take in response to this event, should you find it appropriate to do so.

Other Important Information

RHCC is committed to protecting the information that is entrusted in our care. We are very sorry for any concern or inconvenience caused by this event.

For More Information

If you have further questions in regard to this matter, please contact our dedicated response line at 1-833-796-8636, Monday to Friday 9:00 AM to 11:00 PM (Eastern) and Saturday & Sunday 11:00 AM to 8:00 PM (Eastern), for further information and assistance.

Sincerely,

Robeson Health Care Corporation ("RHCC")

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. 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 or call (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, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. 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 should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online using the above contact information. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online using the above contact information. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.oag.state.md.us/Consumer, and toll-free at (888) 743-0023 or (410) 528-8662.
- **North Carolina Residents:** Office of the Attorney General of North Carolina may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, (919) 716-6400.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by law enforcement.