Robeson Health Care Corporation ("RHCC")
Notice of Data Security Event

At Robeson Health Care Corporation ("RHCC"), we take the privacy and security of patient information seriously. We are providing this notice of a data security event. **To date, we have received no reports or evidence to suggest fraud or identity theft occurred as a result of this event.** However, out of an abundance of caution, we are providing information known to date, the steps we have taken and are taking in response, and additional precautions individuals may take to protect personal information, should they feel it is appropriate to do so.

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 sensitive patient personal information could have been viewed or taken during the period of unauthorized access.

While we reiterate that to date, we have received no reports or evidence to suggest fraud or identity theft occurred as a result of this event, the information potentially accessible on our network could have included names, addresses, Social Security numbers, dates of birth, treatment information/diagnoses, treating physicians, medical record numbers (MRN), patient ID numbers, Medicare/Medicaid numbers, prescription information, health insurance information, and treatment costs.

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.

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 below "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.

If you have further questions in regard to this matter, please contact our dedicated response line at 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. You may also contact us by mail at 60 Commerce Plaza Circle, Pembroke, NC 28372.

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:

- **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.