mwe.com

David Saunders
Attorney at Law
Dsaunders@mwe.com
+1 312 803 8305

December 8, 2023

VIA WEBFORM SUBMISSION

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

Re: Security Incident Notification

Dear Sir or Madame,

I write on behalf of Norton Healthcare, Inc. ("Norton Healthcare"), a not-for-profit healthcare system consisting of eight hospitals in Kentucky and Indiana, with respect to a data security event involving certain personal information of Maine residents. By providing this notice, Norton Healthcare does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

On May 9, 2023, Norton Healthcare discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack. Norton Healthcare notified the Federal Bureau of Investigation and immediately began investigating this incident with the assistance of outside legal counsel and a respected forensic security provider. Norton did not make any ransom payment. Based on our investigation, an unauthorized individual(s) was able to access certain network storage devices between May 7, 2023, and May 9, 2023, but did not access Norton Healthcare's medical record system or Norton MyChart. Between May and November 2023, Norton Healthcare worked to analyze the extent and scope of the incident, and review potentially exfiltrated documents to identify which individuals and types of data were impacted. That process proved to be time-consuming, and did not complete until mid-November 2023.

By mid-November, Norton Healthcare concluded, based on the data available to it, and out of an abundance of caution, that it would be most efficient to notify current (as of May 10, 2023) and former patients, employees, as well as employee dependents and beneficiaries of this incident. That included approximately 385 of Maine residents. The types of data potentially impacted include some or all of the following: name, contact information, Social Security Number, date of birth, health information, insurance information, and medical identification numbers. In some instances, the data may also have included driver's license numbers or other government ID numbers, financial account numbers, and digital signatures.

While its investigation remained ongoing, Norton Healthcare provided updates about the incident on its public website beginning May 11, 2023. Individual notification letters will be sent beginning on December 8, 2023 via regular U.S. mail. Copies of the template notification letters are enclosed. In addition, Norton Healthcare is offering complimentary credit monitoring and identity protection services through Kroll for 24 months. Norton Healthcare also will update the notice on its website and provide media notice.

Norton Healthcare began restoring its systems from secure backups on May 10, 2023. To date, Norton Healthcare has not detected any additional indicators of compromise as its networks have been restored. Norton Healthcare is also enhancing its security safeguards.

If you have any questions, please contact me at 312-803-8305 or dsaunders@mwe.com.

Sincerely,

David Saunders

Enclosure

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We write to inform you about a data security incident at Norton Healthcare, Inc. ("Norton Healthcare") that may have impacted your personal information.

WHAT HAPPENED?

On May 9, 2023, Norton Healthcare discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack. Norton Healthcare notified federal law enforcement and immediately began investigating this incident with the assistance of a respected forensic security provider. Our investigation determined that an unauthorized individual(s) gained access to certain network storage devices between May 7, 2023 and May 9, 2023, but **did not** access Norton Healthcare's medical record system or Norton MyChart. The nature and scope of the incident required time to analyze, and we ultimately determined that your information may have been impacted.

WHAT INFORMATION WAS INVOLVED?

The impacted files contained personal information, primarily about patients, employees, and dependents. The information that may have been impacted varied from person-to-person, but could have included: name, contact information, Social Security number, date of birth, health information, insurance information, and medical identification numbers. In some instances, the data may also have included driver's license numbers or other government ID numbers, financial account numbers, and digital signatures.

WHAT WE ARE DOING

We take safeguarding your information seriously. We promptly notified federal law enforcement and worked with external cybersecurity experts to terminate the unauthorized access. Norton Healthcare is also enhancing its security safeguards.

We have also retained Kroll to provide you with two years of identity monitoring services at no cost, which includes Credit Monitoring, Fraud Consultation, and Identity Theft Restoration services.

- Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
- *You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.*
- Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your identity monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

WHAT YOU CAN DO

We encourage you to enroll in Kroll's identity monitoring services. As always, please remain vigilant and continue reviewing your accounts for unusual activity. You can also review the enclosed steps to help protect your personal information.

FOR MORE INFORMATION

If you have additional questions, please contact us toll-free by calling **(866) 983-5764**, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. We regret any inconvenience this incident may cause you.

Sincerely,

Norton Healthcare

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www. AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to AnnualCredit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney's general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Iowa residents, State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Pro-Tem, Inc. dba PTI Systems is located at 2525 South Shore Boulevard, Suite 401 League City, TX 77573.

For Massachusetts residents, you have the right to obtain a police report if you are the victim of identity theft.

For 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 bureaus 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 the 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 236 Rhode Island residents impacted by this incident.

<<Date>> (Format: Month Day, Year)

Parent or Guardian of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We write to inform you about a data security incident at Norton Healthcare, Inc. ("Norton Healthcare") that may have impacted personal information about your minor.

WHAT HAPPENED?

On May 9, 2023, Norton Healthcare discovered that it was experiencing a cybersecurity incident, later determined to be a ransomware attack. Norton Healthcare notified federal law enforcement and immediately began investigating this incident with the assistance of a respected forensic security provider. Our investigation determined that an unauthorized individual(s) gained access to certain network storage devices between May 7, 2023 and May 9, 2023, but **did not** access Norton Healthcare's medical record system or Norton MyChart. The nature and scope of the incident required time to analyze, and we ultimately determined that your minor's information may have been impacted.

WHAT INFORMATION WAS INVOLVED?

The impacted files contained personal information, primarily about patients, employees, and dependents. The information that may have been impacted varied from person-to-person, but could have included: name, contact information, Social Security number, date of birth, health information, insurance information, and medical identification numbers. In some instances, the data may also have included driver's license numbers or other government ID numbers, financial account numbers, and digital signatures.

WHAT WE ARE DOING

We take safeguarding your minor's information seriously. We promptly notified federal law enforcement and worked with external cybersecurity experts to terminate the unauthorized access. Norton Healthcare is also enhancing its security safeguards.

We have also retained Kroll to provide you with two years of identity monitoring services at no cost, which includes Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration services.

- Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your Minor Identity Monitoring services.
- *You have until <<b2b_text_6(activation deadline)>> to activate your Minor Identity Monitoring services.*
- Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your identity monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

WHAT YOU CAN DO

We encourage you to enroll in Kroll's Minor Identity Monitoring services. As always, please remain vigilant and continue reviewing your accounts for unusual activity. You can also review the enclosed steps to help protect your personal information.

FOR MORE INFORMATION

If you have additional questions, please contact us toll-free by calling **(866) 983-5764**, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. We regret any inconvenience this incident may cause you.

Sincerely,

Norton Healthcare

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your minor's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **Y**ou may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney's general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Iowa residents, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Pro-Tem, Inc. dba PTI Systems is located at 2525 South Shore Boulevard, Suite 401 League City, TX 77573.

For Massachusetts residents, you have the right to obtain a police report if you are the victim of identity theft.

For 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 bureaus 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 the 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 236 Rhode Island residents impacted by this incident.