DATA INCIDENT NOTIFICATION

What Happened

On May 8, 2017, following a forensic investigation by a third-party firm, St. Mark's Surgical Center, LLC (the "Center") discovered that, between April 13 and April 17, 2017, it was the target of a ransomware attack that affected certain electronic files on the Center's server.

What Information Was Involved

The Center's server contains certain data elements of personal information for the Center's patients, such as names, dates of birth, health information, treatment information, and/or Social Security numbers.

What We Are Doing

Although we are not currently aware of any unauthorized use of, access to, or disclosure of the information contained on the Center's server, or of any material loss to the integrity of that information, we are providing notice to all individuals potentially affected by the ransomware pursuant to guidance issued by The Department of Health and Human Services' Office of Civil Rights. Again, we apologize for any inconvenience this may cause you.

Immediately upon learning of the presence of ransomware on our systems, we commenced an investigation to determine its scope, the impact on our systems, and the identity of those affected. We also engaged a third party expert to assist us in recovering the affected data, to help ensure that the server was no longer subject to the ransomware, and to examine whether protected health information or personally identifiable information had been used, accessed, disclosed, acquired, or otherwise compromised by unauthorized parties. As mentioned, we are not aware of any improper use, access, disclosure, acquisition, or compromise of or to the information that was contained on our server. Nonetheless, we are providing this advisory to you and other individuals to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information.

As an added precaution, we have arranged for Epiq to provide to potentially affected individuals 12 months of Equifax Credit Watch credit monitoring and related services at no cost. To find out whether your information was potentially affected by the ransomware attack, and, if you were among those potentially affected, to receive instructions on how to enroll in the free credit monitoring services the Center is providing, please contact (800) 930-3086.

We treat all sensitive patient information in a confidential manner and are proactive in the careful handling of such information. Since the ransomware attack, we have taken a variety of actions to prevent similar situations from occurring in the future. These include installation of a more robust firewall, with unified threat management services; installation of a backup and disaster recovery system that includes active hourly imaging and offsite replication to redundant data centers; and ensuring that all devices are fully updated, and that they are protected by the latest antivirus software.

What You Can Do

To date, we are not aware of any improper use, access, disclosure, acquisition, or compromise of or to the personal information contained on the Center's server. Nonetheless, we are sending this advisory to you and other individuals to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. In addition to enrolling in the credit monitoring service mentioned above, we recommend that you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

    - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your

request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.

- You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you also can report this to the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the email address or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

4. *Iowa Residents:*If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or your state attorney general.

5. *Maryland Residents:* To obtain additional information about avoiding identity theft, please contact the Maryland Attorney General's Office, using the contact information below:

   Maryland Attorney General's Office
   200 St. Paul Place
   Baltimore, MD 21202
   Phone: (410) 576-6300
   Toll-Free (in Maryland): (888) 743-0023
   Website: https://www.oag.state.md.us/contact.htm

6. *North Carolina Residents:* To obtain additional information about avoiding identity theft, please contact the North Carolina Attorney General's Office, using the contact information below:

   Attorney General's Office
   9001 Mail Service Center
   Raleigh, NC 27699-9001
   Phone: (919) 716-6400

Website: http://www.ncdoj.gov/getdoc/714fcea5-4eb0-4558-801d-c12c39bb30c8/DOJ-Contact-Information.aspx

7. *Rhode Island Residents:*To obtain additional information about avoiding identity theft, please contact the Rhode Island Office of the Attorney General, using the contact information below:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
Phone: (401) 274-4400
Website: http://www.riag.ri.gov/home/ContactUs.php

You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may want to place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, please follow these instructions:

- Equifax:

  https://help.equifax.com/s/article/ka137000000DSDjAAO/How-do-I-place-a-security-freeze-on-my-Equifax-credit-file

- Experian:

  http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/

- Transunion:

  https://www.transunion.com/credit-freeze/place-credit-freeze

Mailing addresses for the credit reporting agencies are provided below.

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016

Credit reporting agencies charge a $10.00 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include: (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable, (vi) payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover cards only.)

You can also place a fraud alert with the credit reporting agencies. This will flag your file with a statement that says that you may be a victim of fraud and that creditors should phone you before extending credit. To place a fraud alert on your credit file call the fraud department of one of the three credit reporting agencies – Experian, Equifax, or TransUnion (see above). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for 90 days, and may cancel the fraud alerts at any time.

8. *Vermont Residents:* Below is a check list of suggestions for how to best protect yourself:

a. **Review your bank, credit card, and debit card statements** over the next 12 to 24 months and immediately report any suspicious activity to your bank or credit union.

b. **Monitor your credit reports** with the major credit reporting agencies.

Equifax (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	Experian (888) 397-3742 P.O. Box 2104 Allen, TX 75013 www.experian.com	TransUnion (800) 916-8800 P.O. Box 2000 Chester, PA 19022 www.transunion.com

Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. Call the credit reporting agency at the telephone number on the report if you find: (i) accounts you did not open, (ii) inquiries from creditors that you did not initiate, or (iii) inaccurate personal information, such as home address or Social Security number.

c. If you find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and **file a report of identity theft.** Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.

d. If you find suspicious activity on your credit reports or on your other account statements, **consider placing a fraud alert** on your credit files so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the number below to place fraud alerts with all of the agencies.

Equifax: (800) 525-6285

Experian: (888) 397-3742

TransUnion: (800) 680-7289

e. If you find suspicious activity on your credit reports or on your other account statements, **consider placing a security freeze** on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. A security freeze may cause delay should you wish to obtain credit and may cost some money to get or remove, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. If you have Internet access and would like to learn more about how to place a security freeze on your credit report, please visit the Vermont Attorney General's website at: http://www.atg.state.vt.us/issues/consumer-protection/identity-theft.php

You may also get information about security freezes by contacting the credit bureaus at the following addresses:

Equifax:

https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian:

http://www.experian.com/consumer/security_freeze.html

TransUnion:

http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page

If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at (802) 656-3183 or (800) 649-242 (toll free in Vermont only).

f. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you **check your credit report** for the next two years. Just call one of the numbers in paragraph (b) above to order your reports or to keep a fraud alert in place.

Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at http://www.atg.state.vt.us. Another helpful source is the Federal Trade Commission website, available at http://www.ftc.gov/bcp/edu/microsites/idtheft/.

9. *West Virginia Residents:* You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may want to place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, please follow these instructions:

- Equifax:

  https://help.equifax.com/s/article/ka137000000DSDjAAO/How-do-I-place-a-security-freeze-on-my-Equifax-credit-file

- Experian:

  http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/

- Transunion:

  https://www.transunion.com/credit-freeze/place-credit-freeze

Mailing addresses for the credit reporting agencies are provided below. Credit reporting agencies charge a $5.30 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include: (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable, (vi) payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover cards only.)

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016

You can also place a fraud alert with the credit reporting agencies. This will flag your file with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. To place a fraud alert on your credit file call the fraud department of one of the three credit reporting agencies – Experian, Equifax, or TransUnion (see above). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for 90 days, and may cancel the fraud alerts at any time.

For More Information

If you have questions or concerns, please call (800) 930-3086. Again, we apologize for this situation and any inconvenience it may cause you.

4822-7507-5404, v. 1