McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

November 6, 2018

Via e-mail: SecurityBreach@atg.wa.gov

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Southwest Washington Regional Surgery Center, LLC – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Southwest Washington Regional Surgery Center, LLC ("SWRSC"). I write to provide notification concerning an incident at SWRSC which may affect the security of personal and/or health information of one-thousand six-hundred and ninety (1,690) Washington residents. SWRSC's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, SWRSC does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

SWRSC recently learned that an SWRSC employee email account may have been compromised by an email phishing attack resulting in unauthorized access to the email box between May 27 – August 13, 2018. Upon learning of the issue, SWRSC commenced a prompt and thorough investigation. As part of its investigation, SWRSC has been working very closely with external data privacy and cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual email review, SWRSC discovered on September 25, 2018 that the impacted email account that was accessed contained personal and/or health information of Washington residents. The information that was contained in the account included residents' full names and may have also included one or more of the following: Social Security numbers, driver's license numbers, credit card information, medical diagnostic information, medical treatment information, surgery information, medication information, medical lab information, and/or health insurance information. Not all affected residents had their Social Security numbers impacted by this incident.

To date, SWRSC has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, SWRSC wants to make you (and the affected residents) aware of the incident and explain the steps that have been taken to protected the affected residents from identity theft. The affected residents were provided with written notice of this incident commencing on November 6, 2018, in substantially the same form as the notice

attached hereto. The residents were provided with a toll-free telephone number they can call with questions or concerns. SWRSC is offering a one (1) year of complimentary credit monitoring service to affected residents whose Social Security numbers and/or driver's license numbers were compromised. SWRSC is advising the affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. SWRSC is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files, and obtaining a free credit report. Individuals whose medical diagnostic information, medical treatment information, surgery information, medication information, medical lab information, and/or health insurance information was impacted by this incident are being provided with steps they can take to protect their health information. The affected residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

SWRSC takes its obligation to help protect personal and health information very seriously. SWRSC continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal and health information, including updating passwords and enhancing email access protocols.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

Encl.

Southwest Washington
Regional Surgery Center

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>><<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

November 6, 2018

Dear <<Name 1>>:

I am writing with important information regarding a recent security incident. The privacy and security of the Protected Health Information provided to us is of the utmost importance to Southwest Washington Regional Surgery Center, LLC ("SWRSC"). As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an SWRSC employee email account may have been compromised by an email phishing attack resulting in unauthorized access to the email box between May 27 – August 13, 2018.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external data privacy and cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual email review, we discovered on September 25, 2018 that the impacted email account that was accessed contained some of your Protected Health Information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The impacted email account that was accessed contained some of your Protected Health Information, including your full name, Social Security number, driver's license number, and medical information (diagnosis, treatment, surgery, medications, labs and/or health insurance information).

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks[SM] Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we have also provided information on protecting your health information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information, including updating passwords and enhancing email access protocols.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6 a.m. to 6 p.m. Pacific Time.

Sincerely,

[redacted]

Nancy Molahan
CEO/Administrator
Southwest Washington Regional Surgery Center, LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks[SM] Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code**: [redacted]

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's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Protecting Your Health Information.

We have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.