JOSEPH SALVO
JSALVO@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

June 26, 2020

VIA ELECTRONIC MAIL (DOJ-CPB@DOJ.NH.GOV)
Gordon MacDonald, Attorney General
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Data Security Incident
Our File No: 1211713

To Whom It May Concern:

Our client, Healthcare Fiscal Management, Inc. ("HFMI"), specializes in providing self-pay conversion and Medicaid eligibility verification services for hospital systems, clinics and physician groups, other healthcare providers and their communities. HFMI understands the importance of protecting the personal information provided by its customers and is making this notification to your Office in accordance with applicable law following a recent data security incident.

HFMI provides the aforementioned services to various covered entities throughout the country. In accordance with the Health Insurance Portability and Accountability Act ("HIPAA"), certain covered entities have delegated their notification obligations to HFMI, as its business associate, and HFMI has provided the notifications to the potentially impacted individuals and is providing this notification to you on the covered entity's behalf. The covered entities who have delegated notification obligations to HFMI for purposes of this notification letter are:

- St. Mary's Sacred Heart Hospital, located in Lavonia, Georgia
- St. Mary's Hospital, located in Athens, Georgia
- St. Mary's Good Samaritan Hospital, located in Greensboro, Georgia

On April 13, 2020, HFMI became aware of a data security incident, including ransomware, that impacted portions of its server and data infrastructure. HFMI immediately took its systems offline and undertook efforts to restore its servers to a new hosting provider with additional high-level security mechanisms and monitoring. HFMI thereafter retained a professional forensic investigation firm to determine the nature of the security compromise and identify any individuals whose personal information and/or protected health information may have been compromised.

The forensic investigation determined that first access to HFMI's systems occurred on approximately April 12, 2020, with the ransomware launched on April 13, 2020. The data security incident *may have* resulted in unauthorized access to or acquisition of personal information, including names, date of birth, and Social Security numbers, as well as protected health information, including medical record numbers, account numbers and dates of service that were provided to HFMI in connection with the provision of insurance eligibility services for its clients between November 2019 through April 2020. No direct medical diagnoses or clinical information were part of this breach.

HFMI, at the request of the covered entities, has provided notification to the potentially impacted individuals *via* written and substitute notice beginning on June 26, 2020. A summary of the potentially impacted residents as set forth below:

- St. Mary's Sacred Heart Hospital – two (2) current NH residents
- St. Mary's Hospital – two (2) current NH residents
- St. Mary's Good Samaritan Hospital – one (1) current NH resident

A sample copy of the notification to the New Hampshire residents is attached. As noted in the attachment, HFMI has included in the notification an offer to provide twelve months of one-bureau credit monitoring services to the affected New Hampshire residents. HFMI has also provided notification of this data security incident to the Department of Health and Human Services/Office of Civil Rights on the covered entities' behalf in accordance with HIPAA.

As stated above, following the data security incident, HFMI immediately undertook efforts to restore the impacted servers to a new hosting provider. Backups and other information maintained by HFMI were used to enable near seamless restoration of security and services on the same day. HFMI has retained a forensic investigation firm to thoroughly investigate the incident and has confirmed that the information is no longer in possession of third party(ies) or accessible via the Internet. HFMI is continuing to work closely with leading security experts to identity and implement measures to further strengthen the security of its system to help prevent this from happening in the future.

Should you have any questions or require additional information, please do not hesitate to contact me.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Joseph Salvo

Joseph Salvo, Esq.

Enclosures

HEALTHCARE FISCAL MANAGEMENT, INC.
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

This letter is to notify you of a data security incident at Health Fiscal Management, Inc. ("HFMI") that may have compromised personal information and/or protected health information associated with your treatment from a St. Mary's Health Care System facility or provider between November 2019 and April 2020. This notice provides information about what happened, what HFMI is doing in response, and steps you can take to further protect your information, including whom to call with concerns and the opportunity to sign up for a year of free credit monitoring.

What Happened? On April 13, 2020, HFMI became aware of a data security incident, including ransomware, that impacted portions of its server and data infrastructure. HFMI immediately took its systems offline and undertook efforts to restore its servers to a new hosting provider with additional high-level security mechanisms and monitoring. HFMI thereafter retained a professional forensic investigation firm to determine the nature of the security compromise and identify any individuals whose personal information and/or protected health information may have been compromised.

What Information Was Involved? The forensic investigation determined that first access to HFMI's systems occurred on approximately April 12, 2020, with the ransomware launched on April 13, 2020. The data security incident *may have* resulted in unauthorized access to or acquisition of personal information, including names, date of birth, and Social Security numbers, as well as protected health information, including medical record numbers, account numbers and dates of service that were provided to HFMI in connection with the provision of insurance eligibility services for its clients between November 2019 through April 2020. No direct medical diagnoses or clinical information were part of this breach.

What We Are Doing As stated above, following the data security incident, HFMI immediately undertook efforts to restore the impacted servers to a new hosting provider. Backups and other information maintained by HFMI were used to enable near seamless restoration of security and services on the same day. HFMI has retained a forensic investigation firm to thoroughly investigate the incident and has confirmed that the information is no longer in possession of third party(ies) or accessible via the Internet. HFMI is providing this notice to you in accordance with applicable state law and Health Insurance Portability and Accountability Act (HIPAA) requirements. Please be advised that HFMI is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Additionally, we are offering you a free <<12/24>>-month membership to TransUnion *my*TrueIdentity credit monitoring service. 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. This product also includes various features such as up to $1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. TransUnion *my*TrueIdentity is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft protection and TransUnion *my*TrueIdentity, including instructions on how to activate your complimentary <<12/24>>-month membership, please see the additional information attached to this letter. ***To take advantage of this offer, you must enroll by <<Enrollment Deadline>>.***

What You Can Do We are aware of how important personal information and protected health information is to patients and their loved ones. We encourage you to protect yourself from potential harm associated with this incident by closely monitoring all mail, email, or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements, explanation of benefits statements, and credit reports for unauthorized activity, and to report any such activity or any suspicious contact whatsoever to law enforcement if warranted.

For More Information For further information on steps you can take to prevent against possible fraud or identity theft, please see the attachments to this letter. HFMI understands the importance of protecting your personal information and protected health information, and deeply regrets any concern that this may have caused to you. **Should you have any questions or would like further information regarding the information contained in this letter, do not hesitate to contact (855) 917-3550 between the hours of 9:00 a.m. to 9:00 p.m. EST, Monday through Friday.** In the event that the call-in center is unable to assist you with your questions, we invite you to contact HFMI directly at (877) 353-1187.

Sincerely,

Jack Guggisberg
Owner, Healthcare Fiscal Management, Inc.

Attachment 1: Protecting yourself

Under the Health Insurance Portability and Accountability Act, we advise you that protected health information is defined as individually identifiable information transmitted or maintained in electronic media or any other form or medium, including demographic information collected from an individual, and relates to the past, present, or future physical or mental health conditions, provision of healthcare, or payment for healthcare to an individual.

We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. **Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies.** To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert.

- **Initial Alert:** You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days
- **Extended Alert:** You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a **credit freeze**, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 74021	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Attachment 2: Other Important Information

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon and West Virginia: It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630
www.illinoisattorneygeneral.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.gov

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Connecticut, Massachusetts, Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

TransUnion

Activation Code: <<Activation Code>>

Complimentary <<12/24>> Month *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12/24>> months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<6-digit Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR <<12/24>>-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)