FREEMAN MATHIS & GARY, LLP
Attorneys at Law

550 South Hope Street
Suite 2200
Los Angeles, CA 90071-2631

Tel: 213.615.7000

www.fmglaw.com

Zachariah E. Moura
Partner

Writer's Direct Access
213.615.7055

ZMoura@fmglaw.com

March 6, 2020

VIA U.S. MAIL
Washington State Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notice of Breach in the Security of Personal Information

To Whom it May Concern:

We represent Torrance Memorial Medical Center, which is a medical care provider located in Torrance, California. Pursuant to RCW § 19.255.010(10), enclosed is a copy of an electronic breach notification submitted with the U.S. Office for Civil Rights at the Department of Health and Human Services regarding a breach in the security of protected health information, which affected one resident of the state of Washington.

I believe this provides you with all information necessary for your purposes and to comply with Washington law. However, if anything further is needed, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

ZACHARIAH E. MOURA

Encl.

Breach Tracking Number: **L94ZS4486R**

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification. Your breach notification will be assigned to an OCR staff member for review and appropriate action. If OCR has any questions about the breach notification you submitted, we will contact you directly. Otherwise, you will receive a written response indicating whether or not OCR has accepted your breach notification for investigation.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have any additional information to add to your breach notification, you may call 1-800-368-1019. Please reference the number given by OCR when submitting your breach notification.

* Breach Affecting: 500 or More Individuals
* Report Type: Initial Breach Report

* Are you a Covered Entity filing on behalf of your organization? Yes

---

Covered Entity

* Name of Covered Entity: Torrance Memorial Medical Center
* Type of Covered Entity: Healthcare Provider
* Street Address Line 1: 3330 Lomita Blvd
Street Address Line 2:
* City: Torrance
* State: California
* ZIP: 90505

Covered Entity Point of Contact Information

* First Name: Zachariah * Last Name: Moura
* Email: zmoura@fmglaw.com
* Phone Number: (Include area code): Contact Phones **Phone Number Usage** (213) 615-7055 Work

* Breach Start Date: 06/20/2019 * Breach End Date: 12/13/2019
* Discovery Start Date: 01/06/2020 * Discovery End Date: 02/12/2020
* Approximate Number of Individuals Affected by the Breach: 3448

---

* Type of Breach: Hacking/IT Incident

---

* Location of Breach: Network Server

---

* Type of Protected Health Information Involved in **Clinical**

Breach:	* Clinical Diagnosis/Conditions Other Treatment Information
* Brief Description of the Breach:	On January 6, 2020, Torrance Memorial was notified that a server used by its outside radiology vendor to receive radiological images from Torrance Memorial was unsecured and potentially accessible to unauthorized people. Upon receiving this notice, Torrance Memorial took immediate steps to investigate and address the issue. Our investigation revealed that the server, which is owned and maintained by the vendor at its office, was unsecured from June 20, 2019 until December 13, 2019 when the vendor discovered the issue and secured the server. We discovered that this vendor stores a small volume of patient images on this server temporarily and automatically deletes them from the server every 24 hours. The vendor has confirmed that subsequent scans of its systems show that the server is now secure.
* Safeguards in Place Prior to Breach:	Privacy Rule Safeguards (Training, Policies and Procedures, etc.) Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.) Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.) Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

* Individual Notice Provided Start Date:	03/06/2020	Individual Notice Provided Projected/Expected End Date:	03/06/2020
Was Substitute Notice Required?	No		
Was Media Notice Required?	Yes		
* Select State(s) and/or Territories in which media notice was provided:	California		

* Actions Taken in Response to Breach:	Provided business associate with additional training on HIPAA requirements Revised policies and procedures Other
* Describe Other Actions Taken:	Out of an abundance of caution, we have chosen to notify patients whose records were temporarily stored on the server between June 20, 2019 and December 13, 2019 about this incident. Torrance Memorial takes the security and protection of PHI seriously and we are holding the vendor accountable for raising their security standards to be as stringent as Torrance Memorial's.

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the

HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Zachariah Moura Date: *03/06/2020*

TORRANCE MEMORIAL
A CEDARS-SINAI AFFILIATE
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

March 6, 2020

NOTICE OF DATA BREACH

Dear [redacted]:

Thank you for allowing Torrance Memorial Medical Center ("Torrance Memorial") to serve your healthcare needs. We take patient privacy seriously and as part of that commitment, we are sending you this letter to make you aware of a recent potential data security incident that may have affected your personal information. Please read this letter carefully.

What Happened?

On January 6, 2020, Torrance Memorial was notified that a server used by its outside radiology vendor to receive radiological images from Torrance Memorial was unsecured and potentially accessible to unauthorized people. Upon receiving this notice, Torrance Memorial took immediate steps to investigate and address the issue.

Our investigation revealed that the server, which is owned and maintained by the vendor at its office, was unsecured from June 20, 2019 until December 13, 2019 when the vendor discovered the issue and secured the server. The vendor has confirmed that subsequent scans of its systems show that the server is now secure.

Based on our investigation, we have no evidence that any of your patient images were accessed by any unauthorized persons. We discovered that this vendor stores a small volume of patient images on this server temporarily and automatically deletes them from the server every 24 hours.

What Information Was Involved?

The images and information that was transmitted through the server was for the purpose of providing a professional radiologic reading of patient images. The patient image files on the unsecured server during that time include the patient name, date of birth, gender, medical record number, accession number, and referring physician (if available). The files did **not** contain social security numbers or any financial/payment information.

What We Are Doing

Out of an abundance of caution, we have chosen to notify patients whose records were temporarily stored on the server between June 20, 2019 and December 13, 2019 about this incident. Torrance Memorial takes the security and protection of your personal information seriously and we are holding the vendor accountable for raising their security standards to be as stringent as Torrance Memorial's.

As an added precaution to help protect your information from potential misuse, we are offering identity theft monitoring and restoration services through First Watch ID for a period of 12 months at no cost to you. The identity restoration services are automatically available to you with no enrollment required, but the identity monitoring services do require enrollment. For enrollment instructions and further information about these services, including your personal Verification Code that you will use to enroll, please refer to enclosed documentation.

What You Can Do

We recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, including some information that may be specific to your state of residence.

For More Information

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, please call our dedicated, toll-free incident response hotline at 877-730-4562.

Sincerely,

Mary Goodloe
Torrance Memorial Privacy Officer

TMMC-DFT

First Watch Identity Protection Services

Your Verification Code is: [redacted]

To help safeguard you from misuse of your personal information, we have arranged to have **First Watch ID** monitor your identity for suspicious activity within the United States for 12 months at no cost to you.

First Watch Identity Restoration is automatically available to you with no enrollment required. If a problem arises, simply call 877-817-0173 and provide your Verification Code listed above. Our recovery specialists will help bring your identity back to a "pre-theft" status.

To receive the **First Watch Identity Monitoring Protection Package**, enrollment is required. This free package provides Three Bureau Credit Report Access, Identity Risk Scores, Continuous Identity Monitoring, Account Activity Alerts, Black Web Monitoring, $1 Million Identity Theft Insurance with $0 Deductible, Social Security Statement Access, Lost Wallet/Purse Assistance, Stop Credit Card Offers, E-newsletter, and Monthly Email if No Suspicious Activity is found. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is potentially fraudulent.

You can enroll in this package between now and **June 6, 2020** using the Verification Code listed above. To enroll, go to www.firstwatchid.com, click on the Verification Code button and follow the instructions. Alternatively, you can call 877-817-0173 Monday through Friday between the hours of 9 a.m. and 7 p.m. EST.

Please save this letter in a safe place. Your Verification Code listed above is required when calling First Watch ID Customer Service.

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**
1-866-766-0008	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. Starting September 21, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. 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. Starting September 21, 2018, 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. 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.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or answer security question, you should to promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **California Residents**: Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **Iowa Residents**: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov,(515) 281-5164.
- **Kentucky Residents**: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, (502) 696-5300.
- **Maryland Residents**: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, (888) 743-0023.
- **North Carolina Residents**: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.
- **Oregon Residents**: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **Rhode Island Residents**: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.
- **All US Residents**: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Know Your Rights Under the Fair Credit Reporting Act. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, which you can read about by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf and https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights. These rights include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.