

Exhibit 1

This notice supplements the June 19, 2017 notice to your office of an incident that may affect the security of personal information relating to thirty-one thousand, six hundred and sixty-nine (31,669) California residents. The June 19, 2017 notice to your office is attached here as *Exhibit A*. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Torrance Memorial does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

Nature of the Data Event

On April 20, 2017, Torrance Memorial discovered an email security incident that had taken place on April 18 and 19, 2017. While two email accounts were affected, patient information was only located in one account. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the nature and scope of the incident. The investigation determined that personal information for certain individuals was present in some impacted emails, but it remains unclear whether emails or attachments containing the information were accessed by an unauthorized person or persons.

To date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. However, the email accounts that were accessed through this incident contained sensitive personal information including names, dates of birth, address information, telephone numbers, medical record numbers, Social Security numbers, health insurance information, and other clinical/diagnostic information.

Notice to California Residents

On June 19, 2017, Torrance Memorial began providing written notice of this incident to affected individuals. As we described in our June 19, 2017 notice, we provided notice to thirty-one thousand, six hundred and sixty-nine (31,669) California residents. Based on the ongoing investigation, on July 7, 2017, Torrance Memorial will provide notice to an additional twelve thousand, and ninety-nine (12,099) California residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit B*. Torrance Memorial also published notice of this event on their website beginning on June 19, 2017. This posting is attached hereto as *Exhibit C*. Additionally, on June 19, 2017, Torrance Memorial provided notice to statewide media in California. This notice is attached hereto as *Exhibit D*.

Other Steps Taken and to Be Taken

Upon discovering this incident, Torrance Memorial immediately launched an investigation, with the assistance of third party forensic investigators, to determine the nature and scope of this incident and to identify those that may be affected.

Torrance Memorial is providing all potentially affected individuals access to one (1) free year of credit monitoring services and identity restoration services and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Torrance Memorial is providing potentially impacted individuals with guidance on

how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Torrance Memorial has provided notice of this incident to the California Department of Public Health and will also be providing notice of this incident to the U.S. Department of Health and Human Services, as well as to certain state official as required by law.

EXHIBIT A

State of California  Department of Justice

OFFICE of the ATTORNEY GENERAL

DATA BREACH SUBMISSION CONFIRMATION

Data Breach Report (SB24) *Submitted Breach Notification Sample* has been created.

On behalf of the Office of the Attorney General, I would like to thank you for your submission.

State of California ~ Department of Justice
OFFICE of the ATTORNEY GENERAL

CREATE DATA BREACH REPORT (SB24)

The answer you entered for the CAPTCHA was not correct.

Is the organization a small business, according to the Small Business Administrator? field is required.

This submission is required by California Civil Code s. 1798.29(e); California Civil Code s. 1798.82(f)

Note: This form is only for use by businesses and state and local government agencies, which are required to submit a sample notice if they experience a breach of personal information involving more than 500 California residents.

If you are a consumer who wishes to file a complaint, please use our online [complaint form](#).

SECTION 1 - ATTACH SECURITY BREACH NOTIFICATION SAMPLE

Sample of Notice

California Civil Code s. 1798.29(e) and s. 1798.82(f) provide that "...A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of [Section 6254](#) of the Government Code.

Click browse button to select file and then click upload to attach the file.

[Show row weights](#)

File information

Display

Operations

 [Torrance - CA Form.pdf](#) (234.44 KB)

Description



Remove

The description may be used as the label of the link to the file.

SECTION 2 - INFORMATION FOR LAW ENFORCEMENT PURPOSES

The information provided in SECTION 2 is for DOJ use.

Organization Name

Address

City

State

Zip Code

[Show row weights](#)

Date(s) of Breach (if known)

CAPTCHA

This question is for testing whether you are a human visitor and to prevent automated spam submissions.

I'm not a robot

reCAPTCHA
Privacy - Terms

Date(s) of Breach (if known)

Date

2017-04-18

E.g., 2017-06-19

Date(s) of Breach (if known) 2

Date

2017-04-19

E.g., 2017-06-19

Add another Date

Show row weights

Date(s) of Discovery of Breach

Date(s) of Discovery of Breach

Date

2017-04-20

E.g., 2017-06-19

Add another Date

Show row weights

Date(s) Individual Notice Provided to Consumers

Date(s) Individual Notice Provided to Consumers

Date

2017-06-19

E.g., 2017-06-19

Add another Date

Was notification delayed because of a law enforcement investigation?

- N/A
- No
- Yes

Type of Personal Information Involved in the Breach

- None -

Social Security Number Information

Driver's License number or California ID Card number information

Financial Information (e.g. account number, credit or debit card numbers)

("Press Ctrl for Multiple Selections") If selecting an "Other" category, please describe the information in detail in the Description section below.

Brief Description of the Breach

See Exhibit 1.

Please include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected information involved in the breach.

Report Type

- N/A
- Addendum to Previous Report
- Initial Breach Report

Breach Affecting

- N/A
- Fewer Than 500 Individuals
- 500 or More Individuals

Approximate Number of Individuals Affected by the Breach

32,499

Approximate Number of Californians Affected by the Breach

31,669

Type of Entity

- EDU - Educational Institutions
- GOV - Government and Military
- MED - Healthcare - Medical Providers
- NGO - Nonprofit organizations

(*Press Ctrl for Multiple Selections*)

Is the organization a small business, according to the Small Business Administrator? *

- Yes
- No
- Unsure

(See the Small Business Administration's standards for defining a "small business": www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf.)

Type of Breach

- Unintended disclosure
- Hacking or malware
- Payment Card Fraud
- Insider
- Physical loss
- Portable device
- Stationary device
- Other

If Type of Breach is "Other" please describe the type of breach here

Phishing

Location of Breached Information

E-mail

If Location of Breached Information is "Other" please describe the location here

Was Substitute Notice Given?

- N/A
- No
- Yes

Was Media Notice Given?

- N/A
- No
- Yes

Name of company contact whom the Attorney General may contact for further information

Edward Finn

Telephone Number

267-930-4776

Email address

efinn@mullen.law

Was a law enforcement agency notified regarding the breach?

- N/A
- No
- Yes

If Yes, name of law enforcement agency and contact name and number

Federal Bureau of Investigation

Was a police report filed?

- N/A
- No
- Yes

If yes, police report number

Submit form

Submit

The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Torrance Memorial does not waive any rights or defenses regarding the applicability of California law or personal jurisdiction.

Nature of the Data Event

On April 20, 2017, Torrance Memorial discovered an email security incident that had taken place on April 18 and 19, 2017. The incident allowed access to two email accounts that contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the nature and scope of the incident. The investigation determined that personal information for certain individuals was present in some impacted emails, but it remains unclear whether emails or attachments containing the information were accessed by an unauthorized person or persons.

To date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. However, the email accounts that were accessed through this incident contained sensitive personal information including names, dates of birth, address information, telephone numbers, medical record numbers, Social Security numbers, health insurance information, and other clinical/diagnostic information.

Notice to California Residents

On June 19, 2017, Torrance Memorial will begin providing written notice of this incident to affected individuals, which includes thirty-one thousand, six hundred, and sixty-nine (31,669) California residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*. Torrance Memorial also published notice of this event on their website beginning on June 19, 2017. This posting is attached hereto as *Exhibit B*. Additionally, on June 19, 2017, Torrance Memorial provided notice to statewide media in California. This notice is attached hereto as *Exhibit C*.

Other Steps Taken and To Be Taken

Upon discovering this incident, Torrance Memorial immediately launched an investigation, with the assistance of third party forensic investigators, to determine the nature and scope of this incident and to identify those that may be affected.

Torrance Memorial is providing all potentially affected individuals access to one (1) free year of credit monitoring services and identity restoration services and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Torrance Memorial is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Torrance Memorial has provided notice of this incident to the California Department of Public Health and will also be providing notice of this incident to the U.S. Department of Health and Human Services, as well as to certain state official as required by law.



Return Mail Processing
P.O. Box 190
Claysburg, PA 16625-0190

June 19, 2017

##C8739-L02-0123456 0001 00000001 *****9-OELZZ 123
SAMPLE A SAMPLE



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



Re: Notice of Data Breach

Dear Sample A Sample:

I write to make you aware of a recent data security incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On April 20, 2017, Torrance Memorial Medical Center (“Torrance Memorial”) discovered that it had experienced an email security incident that allowed access to two staff members’ email accounts which contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of this incident. The investigation determined that personal information for certain individuals was present in some impacted emails. Based upon available forensic evidence, it appears these cyber attacks took place on April 18 and 19, 2017.

What Information Was Involved? While Torrance Memorial’s investigation is ongoing, to date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. Based on the investigation, we have determined that the information affected may include your: name, Social Security number, address, health insurance information, date of birth, and treatment/diagnostic information.

What We Are Doing. We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information on our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We will also be notifying state officials, as required by law.

As an added precaution, we are also offering you access to one (1) year of credit monitoring and identity theft restoration services through Experian at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. More information on these services can be found in the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.”

What You Can Do. Please review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.” You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877)238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays) and provide reference number **9995061317** when calling.

Again, Torrance Memorial takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Mary Goodloe
Torrance Memorial Privacy Officer

0123456



STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or fraud.

Credit Monitoring. As an added precaution, we are offering you access to one year of identity theft protection and credit monitoring services through Experian at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to do so. More information on the services being offer and information on how to enroll can be found below:

Fraud Detection Tool. We encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2017** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/creditone
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **September 30, 2017**. Be prepared to provide engagement number **DB02248** as proof of eligibility for the identity restoration services by Experian.

Identity Restoration. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

Terms & Conditions are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional details regarding your 12-Month Experian IdentityWorks Membership

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

- **\$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please refer to www.ExperianIDWorks.com/restoration for more information.

We encourage you to enroll in the credit monitoring services we are offering as we are not able to act on your behalf to enroll you in the credit monitoring service.

Monitor Your Accounts.

Credit Reports & Explanation of Benefits. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

0123456



² 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.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Information on this event may be found at <http://www.torrancememorial.org/>.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.



**TORRANCE MEMORIAL
MEDICAL CENTER**

Return Mail Processing
P.O. Box 190
Claysburg, PA 16625-0190

June 19, 2017

##C8739-L03-0123456 0001 00000001 *****9-OELZZ 123
NEXT OF KIN OF SAMPLE A SAMPLE



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



Re: Notice of Data Breach

To the Next of Kin of Sample A Sample:

I write to make you aware of a recent data security incident that may affect the security of your loved one’s personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your loved one’s personal information, should you feel it is appropriate to do so.

What Happened? On April 20, 2017, Torrance Memorial Medical Center (“Torrance Memorial”) discovered that it had experienced an email security incident that allowed access to two staff members' email accounts which contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of this incident. The investigation determined that personal information for certain individuals was present in some impacted emails. Based upon available forensic evidence, it appears these cyber attacks took place on April 18 and 19, 2017.

What Information Was Involved? While Torrance Memorial’s investigation is ongoing, to date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. Based on the investigation, we have determined that the information affected may include your loved one’s: name, Social Security number, address, health insurance information, date of birth, and treatment/diagnostic information.

What We Are Doing. We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information on our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We will also be notifying state officials, as required by law.

What You Can Do. Please review the enclosed “Steps You Can Take to Protect Your Loved One’s Information.”

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877)238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays) and provide reference number **9995061317** when calling.

0123456

Again, Torrance Memorial takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.



Sincerely,

Mary Goodloe
Torrance Memorial Privacy Officer

Steps You Can Take to Protect Your Loved One's Information

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss

Monitoring Accounts: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements, free credit reports, medical bills, and health insurance statements regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your loved one's name and other information. Report all suspicious or fraudulent charges to your loved one's account and insurance providers. If your loved one did not receive regular Explanation of Benefits statements, you can contact your loved one's health plan and request them to send such statements following the provision of services.

In addition, there are steps you can take to protect your loved one's credit file. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

You may also contact the three major credit bureaus directly to request a free copy of this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the credit report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. Contact information for the three major credit bureaus is as follows:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Information on this event may be found at <http://www.torrancememorial.org/>.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

0123456



NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

On April 20, 2017, Torrance Memorial Medical Center (Torrance Memorial) discovered an email security incident that had taken place on April 18 and 19, 2017. The incident allowed access to two email accounts that contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the nature and scope of the incident. The investigation determined that personal information for certain individuals was present in some impacted emails, but it remains unclear whether emails or attachments containing the information were accessed by an unauthorized person or persons.

We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information on our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We will also be notifying state officials, as required by law.

FREQUENTLY ASKED QUESTIONS

Q: What happened? Torrance Memorial was targeted by a cyberattack that allowed an unauthorized actor(s) access to two email accounts that contained work-related reports. To date, we have no evidence of any actual or attempted misuse of information as a result of this incident. Torrance Memorial considers matters of security and privacy of the utmost importance and we are taking proactive steps to address this incident.

Q: What information may have been affected by this incident? Again, to date, we have no evidence of any actual or attempted misuse of information as a result of this incident. However, the email accounts that were accessed through this incident contained sensitive personal information including names, dates of birth, address information, telephone numbers, medical record numbers, Social Security numbers, health insurance information, and other clinical/diagnostic information.

Q: How will I know if I am affected by this incident? On June 19, 2017, Torrance Memorial began mailing notice letters to individuals whose data was present on the affected systems for whom Torrance has address information. Torrance Memorial will continue the notification process should additional individuals be determined to be potentially impacted. In the meantime, if you believe you may be impacted, our dedicated assistance line can be reached at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays). Please provide reference number **9995061317** when calling.

Q: Is Torrance Memorial providing impacted individuals access to credit monitoring services? Yes, Torrance Memorial is providing potentially impacted individuals access to credit monitoring services. Information on these services is included in the notice letter mailed to individuals whose information was on the affected systems for whom Torrance Memorial has address information.

Q: What may I do to protect my information?

Monitor Your Accounts.

Credit Reports & Explanation of Benefits. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit

www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

NOTICE TO MEDIA

FOR IMMEDIATE RELEASE

Torrance Memorial Experiences Phishing Incident

Torrance, CA (June 19, 2017) – On April 20, 2017, Torrance Memorial Medical Center (Torrance Memorial) discovered an email security incident that had taken place on April 18 and 19, 2017. The incident allowed access to two email accounts which contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the nature and scope of the incident. The investigation determined that personal information for certain individuals was present in some impacted emails, but it remains unclear whether emails or attachments containing the information were accessed by an unauthorized person or persons.

Torrance Memorial's investigation is ongoing and the incident has been reported to pertinent regulatory bodies, including the California Department of Public Health, the U.S. Department of Health and Human Services, and the Federal Bureau of Investigation. To date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. However, the email accounts that were accessed through this incident contained sensitive personal information including names, dates of birth, address information, telephone numbers, medical record numbers, Social Security numbers, health insurance information, and other clinical/diagnostic information.

On June 19, 2017, Torrance Memorial began mailing notice letters to potentially impacted individuals. Torrance Memorial has offered these individuals access to credit monitoring and identity theft protection services for one year without charge. Torrance Memorial encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor free credit reports and explanation of benefits forms for suspicious activity. Torrance Memorial's notification to potentially impacted individuals includes information such as obtaining a free credit report annually from each of the three major credit reporting bureaus by visiting www.annualcreditreport.com, calling 877-322-8228, or contacting the three major credit bureaus directly at: **Equifax**, P.O. Box 105069, Atlanta, GA, 30348, 800-525-6285, www.equifax.com; **Experian**, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; **TransUnion**, P.O. Box 2000, Chester, PA 19016, 800-680-7289, www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Torrance Memorial considers matters of security and privacy of the utmost importance and has set up a call center to answer questions from those who might be impacted by this incident. Our dedicated assistance line can be reached at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays). Please provide reference number **9995061317** when calling. Additional information on how potentially impacted individuals can protect themselves can also be found at Torrance Memorial's website at www.TorranceMemorial.org/notification. Instances of known or suspected identity theft should also be reported to law enforcement or the individual's state Attorney General.

EXHIBIT B



TORRANCE MEMORIAL
MEDICAL CENTER
 3330 Lomita Blvd
 Torrance, CA 90505

July 7, 2017

##C9153-L02-0123456 0001 00000001 *****9-OELZZ 123
 SAMPLE A SAMPLE



APT ABC
 123 ANY ST
 ANYTOWN, US 12345-6789



Re: Notice of Data Breach

Dear Sample A Sample:

I write to make you aware of a recent data security incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On April 20, 2017, Torrance Memorial Medical Center (“Torrance Memorial”) discovered that it had experienced an email security incident that allowed access to a staff member’s email account which contained work-related reports. While two email accounts were affected, patient information was only located in one account. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of this incident. The investigation determined that personal information for certain individuals was present in one email account. Based upon available forensic evidence, it appears these cyber attacks took place on April 18 and 19, 2017.

What Information Was Involved? While Torrance Memorial’s investigation is ongoing, to date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. Based on the investigation, we have determined that the information affected may include your: name, Social Security number, address, health insurance information, date of birth, and treatment/diagnostic information.

What We Are Doing. We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information in our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We are notifying state officials, as required by law.

As an added precaution, we are also offering you access to one (1) year of credit monitoring and identity theft restoration services through Experian at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. More information on these services can be found in the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.”

What You Can Do. Please review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.” You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays) and provide reference number **9995061317** when calling.

Again, Torrance Memorial takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Mary Goodloe
 Torrance Memorial Privacy Officer

0123456



STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or fraud.

Credit Monitoring. As an added precaution, we are offering you access to one year of identity theft protection and credit monitoring services through Experian at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to do so. More information on the services being offer and information on how to enroll can be found below:

Fraud Detection Tool. We encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2017** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/creditone>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **September 30, 2017**. Be prepared to provide engagement number **DB02450** as proof of eligibility for the identity restoration services by Experian.

Identity Restoration. If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

Terms & Conditions are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional details regarding your 12-Month Experian IdentityWorks Membership

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please refer to www.ExperianIDWorks.com/restoration for more information.

We encourage you to enroll in the credit monitoring services we are offering as we are not able to act on your behalf to enroll you in the credit monitoring service.

Monitor Your Accounts.

Credit Reports & Explanation of Benefits. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

0123456



² 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.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Information on this event may be found at <http://www.torrancememorial.org/>.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.



TORRANCE MEMORIAL
MEDICAL CENTER
 3330 Lomita Blvd
 Torrance, CA 90505

July 7, 2017

##C9153-L04-0123456 0001 00000001 *****9-OELZZ 123

NEXT OF KIN OF SAMPLE A SAMPLE



APT ABC
 123 ANY ST
 ANYTOWN, US 12345-6789



Re: Notice of Data Breach

To the Next of Kin of Sample A Sample:

I write to make you aware of a recent data security incident that may affect the security of your loved one’s personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your loved one’s personal information, should you feel it is appropriate to do so.

What Happened? On April 20, 2017, Torrance Memorial Medical Center (“Torrance Memorial”) discovered that it had experienced an email security incident that allowed access to a staff member’s email account which contained work-related reports. While two email accounts were affected, patient information was only located in one account. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of this incident. The investigation determined that personal information for certain individuals was present in one email account. Based upon available forensic evidence, it appears these cyber attacks took place on April 18 and 19, 2017.

What Information Was Involved? While Torrance Memorial’s investigation is ongoing, to date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. Based on the investigation, we have determined that the information affected may include your loved one’s: name, Social Security number, address, health insurance information, date of birth, and treatment/diagnostic information.

What We Are Doing. We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information in our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We are notifying state officials, as required by law.

What You Can Do. Please review the enclosed “Steps You Can Take to Protect Your Loved One’s Information.”

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays) and provide reference number **9995061317** when calling.

0123456



Again, Torrance Memorial takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink that reads "Mary Goodloe". The signature is written in a cursive style with a large, prominent "M" and "G".

Mary Goodloe
Torrance Memorial Privacy Officer

Steps You Can Take to Protect Your Loved One's Information

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

Monitoring Accounts: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements, free credit reports, medical bills, and health insurance statements regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your loved one's name and other information. Report all suspicious or fraudulent charges to your loved one's account and insurance providers. If your loved one did not receive regular Explanation of Benefits statements, you can contact your loved one's health plan and request them to send such statements following the provision of services.

In addition, there are steps you can take to protect your loved one's credit file. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

You may also contact the three major credit bureaus directly to request a free copy of this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the credit report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. Contact information for the three major credit bureaus is as follows:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

0123456



For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Information on this event may be found at <http://www.torrancememorial.org/>.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.



TORRANCE MEMORIAL
MEDICAL CENTER
 3330 Lomita Blvd
 Torrance, CA 90505

July 7, 2017

##C9153-L06-0123456 0001 00000001 *****9-OELZZ 123
 PARENT OR GUARDIAN OF SAMPLE A SAMPLE



APT ABC
 123 ANY ST
 ANYTOWN, US 12345-6789



Re: Notice of Data Breach

Dear Parent or Guardian of Sample A Sample:

I write to make you aware of a recent data security incident that may affect the security of your minor’s personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your minor’s personal information, should you feel it is appropriate to do so.

What Happened? On April 20, 2017, Torrance Memorial Medical Center (“Torrance Memorial”) discovered that it had experienced an email security incident that allowed access to a staff member’s email account which contained work-related reports. While two email accounts were affected, patient information was only located in one account. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of this incident. The investigation determined that personal information for certain individuals was present in one email account. Based upon available forensic evidence, it appears these cyber attacks took place on April 18 and 19, 2017.

What Information Was Involved? While Torrance Memorial’s investigation is ongoing, to date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. Based on the investigation, we have determined that the information affected may include your minor’s: name, Social Security number, address, health insurance information, date of birth, and treatment/diagnostic information.

What We Are Doing. We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information in our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We are notifying state officials, as required by law.

As an added precaution, we are also offering your minor access to one (1) year of identity monitoring and identity theft restoration services through Experian at no cost to you. We encourage you to enroll your minor in these services, as we are not able to act on your behalf to do so. More information on these services can be found in the enclosed “Steps You Can Take to Protect Your Minor’s Information.”

What You Can Do. Please review the enclosed “Steps You Can Take to Protect Your Minor’s Information.” You can also enroll your minor to receive the free identity monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays) and provide reference number **9995061317** when calling.

Again, Torrance Memorial takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Mary Goodloe
 Torrance Memorial Privacy Officer

0123456



Steps You Can Take to Protect Your Minor's Information

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

Credit Monitoring. As an added precaution, we are offering you access to one year of fraud detection services for your minor through Experian at no cost to you. We encourage you to enroll your minor in these services, as we are not able to act on your behalf to do so. More information on the services being offer and information on how to enroll can be found below:

Fraud Detection Tool. We also encourage you to activate the fraud detection tools for your minor available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with internet surveillance, and identity theft insurance at no cost to you upon enrollment. To start monitoring your minor's personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2017** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/minorplusone>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration for your minor, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by September 30, 2017. Be prepared to provide engagement number **DB02451** as proof of eligibility for the identity restoration services by Experian.

Identity Restoration. If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; and assisting you with contacting government agencies to help restore your minor's identity to his/her proper condition). Please note that this offer is available to your minor for one-year from the date of this letter and does not require any action on your part at this time.

Terms & Conditions Terms and Conditions are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional details regarding your 12-Month Experian IdentityWorks Membership

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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 Insurance¹:** Provides coverage for certain costs and unauthorized electronicfund transfers.

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). Refer to www.ExperianIDWorks.com/restoration for this information.

We encourage you to enroll your minor in the credit monitoring services we are offering as we are not able to act on your behalf to do so.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing applicable account statements and monitoring your minor’s credit reports (should they maintain credit files) and explanation of benefits forms for suspicious activity. Under U.S. law, adults are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of a credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your minor’s file (should such credit file exist) that alerts creditors to take additional steps to verify identity prior to granting credit in your minor’s name. Note, however, that because it tells creditors to follow certain procedures to protect your minor, it may also delay in the ability to obtain credit while the agency verifies identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts on the file. Should you wish to place a fraud alert, or should you have any questions regarding a credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your minor’s credit file (should such files exist). A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests your minor may make for new loans, credit mortgages, employment, housing, or other services. If your minor has been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your minor’s credit files. In order to request a security freeze, you will need to supply your minor’s full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of a state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

0123456



¹ 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.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect your minor against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Information on this event may be found at <http://www.torrancememorial.org/>.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

EXHIBIT C

NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

On April 20, 2017, Torrance Memorial Medical Center (Torrance Memorial) discovered an email security incident that had taken place on April 18 and 19, 2017. The incident allowed access to two email accounts that contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the nature and scope of the incident. The investigation determined that personal information for certain individuals was present in some impacted emails, but it remains unclear whether emails or attachments containing the information were accessed by an unauthorized person or persons.

We take the security of personal information in our care very seriously. We have security measures in place to protect data in our care and we are also working to implement additional safeguards and provide additional training to our staff on safeguarding the privacy and security of information on our systems. We have reported this incident to the California Department of Public Health, the U.S. Department of Health and Human Services, and the FBI. We will also be notifying state officials, as required by law.

FREQUENTLY ASKED QUESTIONS

Q: What happened? Torrance Memorial was targeted by a cyberattack that allowed an unauthorized actor(s) access to two email accounts that contained work-related reports. To date, we have no evidence of any actual or attempted misuse of information as a result of this incident. Torrance Memorial considers matters of security and privacy of the utmost importance and we are taking proactive steps to address this incident.

Q: What information may have been affected by this incident? Again, to date, we have no evidence of any actual or attempted misuse of information as a result of this incident. However, the email accounts that were accessed through this incident contained sensitive personal information including names, dates of birth, address information, telephone numbers, medical record numbers, Social Security numbers, health insurance information, and other clinical/diagnostic information.

Q: How will I know if I am affected by this incident? On June 19, 2017, Torrance Memorial began mailing notice letters to individuals whose data was present on the affected systems for whom Torrance has address information. Torrance Memorial will continue the notification process should additional individuals be determined to be potentially impacted. In the meantime, if you believe you may be impacted, our dedicated assistance line can be reached at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays). Please provide reference number **9995061317** when calling.

Q: Is Torrance Memorial providing impacted individuals access to credit monitoring services? Yes, Torrance Memorial is providing potentially impacted individuals access to credit monitoring services. Information on these services is included in the notice letter mailed to individuals whose information was on the affected systems for whom Torrance Memorial has address information.

Q: What may I do to protect my information?

Monitor Your Accounts.

Credit Reports & Explanation of Benefits. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit

www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Torrance Memorial is located at 3330 Lomita Blvd. Torrance CA, 90505.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or 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.

Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

EXHIBIT D

NOTICE TO MEDIA

FOR IMMEDIATE RELEASE

Torrance Memorial Experiences Phishing Incident

Torrance, CA (June 19, 2017) – On April 20, 2017, Torrance Memorial Medical Center (Torrance Memorial) discovered an email security incident that had taken place on April 18 and 19, 2017. The incident allowed access to two email accounts which contained work-related reports. Torrance Memorial immediately launched an investigation, which included working with third-party forensic investigators, to determine the nature and scope of the incident. The investigation determined that personal information for certain individuals was present in some impacted emails, but it remains unclear whether emails or attachments containing the information were accessed by an unauthorized person or persons.

Torrance Memorial's investigation is ongoing and the incident has been reported to pertinent regulatory bodies, including the California Department of Public Health, the U.S. Department of Health and Human Services, and the Federal Bureau of Investigation. To date, Torrance Memorial has no evidence of any actual or attempted misuse of information as a result of this incident. However, the email accounts that were accessed through this incident contained sensitive personal information including names, dates of birth, address information, telephone numbers, medical record numbers, Social Security numbers, health insurance information, and other clinical/diagnostic information.

On June 19, 2017, Torrance Memorial began mailing notice letters to potentially impacted individuals. Torrance Memorial has offered these individuals access to credit monitoring and identity theft protection services for one year without charge. Torrance Memorial encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor free credit reports and explanation of benefits forms for suspicious activity. Torrance Memorial's notification to potentially impacted individuals includes information such as obtaining a free credit report annually from each of the three major credit reporting bureaus by visiting www.annualcreditreport.com, calling 877-322-8228, or contacting the three major credit bureaus directly at: **Equifax**, P.O. Box 105069, Atlanta, GA, 30348, 800-525-6285, www.equifax.com; **Experian**, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; **TransUnion**, P.O. Box 2000, Chester, PA 19016, 800-680-7289, www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Torrance Memorial considers matters of security and privacy of the utmost importance and has set up a call center to answer questions from those who might be impacted by this incident. Our dedicated assistance line can be reached at (877) 238-2074, Monday through Friday, 9 am to 7 pm EST (Closed on U.S. observed holidays). Please provide reference number **9995061317** when calling. Additional information on how potentially impacted individuals can protect themselves can also be found at Torrance Memorial's website at www.TorranceMemorial.org/notification. Instances of known or suspected identity theft should also be reported to law enforcement or the individual's state Attorney General.