Bob Ferguson

ATTORNEY GENERAL OF WASHINGTON

University of Washington Division • Box 359475
Seattle WA 98195-9475 • Phone (206) 543-4150 • Fax (206) 543-0779

February 20, 2019

Via email (SecurityBreach@atg.wa.gov)

Attorney General Bob Ferguson
Office of the Attorney General
State of Washington
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504-0100

RE: Incident Notification

Dear Mr. Ferguson:

I am writing on behalf of the University of Washington Medical Center to provide a courtesy notice regarding a security incident. Although no "personal information" as defined in RCW 42.56.590 was disclosed in the incident, please see the enclosed notice provided to the Secretary of Health and Human Services. Approximately 894,272 Washington residents were affected. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

DAVID M. KERWIN
Assistant Attorney General
(206) 543-4150

Enclosure

Breach Tracking Number: **ZF9TTX6LGC**

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:	UW Medicine
* Type of Covered Entity:	Healthcare Provider
* Street Address Line 1:	Box 358049
Street Address Line 2:	
* City:	Seattle
* State:	Washington
* ZIP:	98195

Covered Entity Point of Contact Information

* First Name: James * Last Name: Mathis
* Email: comply@uw.edu
* Phone Number: (Include area code): Contact Phones

Phone Number Usage	
(206) 543-3098	Work

* Breach Start Date: 12/04/2018 * Breach End Date: 01/10/2019
* Discovery Start Date: 12/26/2018 * Discovery End Date: 01/07/2019
* Approximate Number of Individuals Affected by the Breach: 974351

---

* Type of Breach:	Hacking/IT Incident
* Location of Breach:	• Network Server
* Type of Protected Health Information Involved in Breach:	• **Clinical** • **Demographic** * Clinical • Other Treatment Information * Demographic • Name • Other Identifier
* Brief Description of the Breach:	On December 4, 2018, an error in a database configuration exposed internal files containing PHI to the internet. Specifically, the files contained information that was uploaded into UW Medicine's database used for tracking disclosures as required by the accounting of disclosures provision of the Privacy Rule. UW Medicine immediately removed access to the files and worked with Google to permanently remove the files from their cache. UW Medicine confirmed no other internet search engine cached the files.
* 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:	02/19/2019	Individual Notice Provided Projected/Expected End Date:	02/22/2019
Was Substitute Notice Required?	Yes		
	10 or more		
Was Media Notice Required?	Yes		

* Select State(s) and/or Territories in which media notice was provided:	• Alaska • Arizona • California • Colorado • Florida • Georgia • Hawaii • Idaho • Illinois • Massachusetts • Maryland • Michigan • Minnesota • Missouri • Montana • North Carolina • New Jersey • New Mexico • Nevada • New York • Ohio • Oregon • Pennsylvania • Texas • Utah • Virginia • Washington • Wisconsin

---

* Actions Taken in Response to Breach:	• Revised policies and procedures • Took steps to mitigate harm • Trained or retrained workforce members • Other
* Describe Other Actions Taken:	On Dec. 26, 2018, UW Medicine became aware of a configuration error on a website server that made protected internal files available and visible by search on the internet on Dec. 4, 2018. The files contained PHI about reporting that UW Medicine is legally required to track, such as reporting to various regulatory bodies in compliance with Washington state requirements. When we learned of the exposure of the files to the internet, we took immediate steps to remove the information from the site and to work with Google to remove any of its cached files. At this time, there is no evidence that there has been any attempted misuse of the information exposed in this incident. The files contained patients' names, medical record numbers, and a description and purpose of various information. The files did not contain any medical records, patient financial information, or

any Social Security numbers. Based on the results of our internal investigation, we are in the process of distributing letters to approximately 974,000 affected patients. While UW Medicine is contacting this large group of patients out of an abundance of caution, a much smaller number of patients were potentially affected by the breach. Approximately 2,100 patients had reports regarding their sensitive test results (but not the test results themselves) accessed. Approximately 69,000 patients had sensitive PHI cached by Google, with no evidence of any further inappropriate access. No evidence or reasonable likelihood exists that any other patient outside of that group had their sensitive PHI inappropriately accessed. Because of the type of information that was potentially exposed (e.g., no Social Security numbers, no account numbers, no payment methods), there is an extremely low to nonexistent chance of identity theft resulting from the breach. UW Medicine has notified the media as required, has posted information to a dedicated website and has made available a toll-free number for patients to call with questions. UW Medicine is taking significant steps to address issues of formalizing and centralizing policy and procedure, especially around change management. Until permanent procedures are implemented, the ability to make changes to the public web server has been suspended. Any emergency changes must receive a leadership review at the Director level. Any change to the server which potentially involves any access to PHI, or any public access at all, is subjected to additional security review. Significantly, UW Medicine has retained Huntzinger Consulting to review its entire change management process. This analysis will begin within two weeks and will take several months. We expect an emphasis on unification and strengthening of change management processes. There will also be an emphasis on strength of testing prior to implementation of server changes. UW Medicine has also re -evaluated risk questions utilized during risk reviews and has added queries targeted to configuration class errors. UW Medicine is meticulously reviewing all public facing websites. This will take 2 or 3 more weeks to complete. A review of server settings confirms there is no additional information which has been exposed to the internet. All server level directory browsing has been confirmed disabled. All server subdirectory folders have been removed to a separate root directory. In implementing new technical safeguards, UW Medicine is exploring the implementation of Data Loss Prevention, a tool that monitors all data transfer and triggers appropriate alerts. It is also in process of considering various vulnerability and penetration testing services. In terms of training, communications have been made to all relevant personnel regarding immediate policy and procedure changes. Comprehensive training will follow the consultant's report.

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: James Mathis Date: *02/20/2019*