Seattle Indian Health Board

For the Love of Native People

May 9, 2017

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Notification to Attorney General

To Whom It May Concern:

As required under the RCS 19.255.010, I am providing notification of a breach of our email system at the Seattle Indian Health Board (SIHB).

On August 10, 2016, SIHB experienced an unknown intruder attack on an employee email account. After approximately four hours, the SIHB Information Technology (IT) department was able to shut down the unauthorized access. SIHB immediately launched an investigation to evaluate the extent of the incident. The internal investigation indicated that the risk of exposure of patient information was low given the intruder's behavior while in the account. However, because SIHB cannot confirm that absolutely no patient information was accessed, SIHB made the decision to notify its patients (approximately 4,579) and Office of Civil Rights (OCR) out of an abundance of caution.

Although the breach occurred on August 10, 2016 and SIHB did report the breach to OCR and sent a letter out to our patients within the deadline, we failed to provide notification to the Attorney General. This requirement has only recently come to my attention and that is why you are receiving the information now. This was an oversite on our part but I want to assure you that we have complied in every other aspect under the law (including notification to local national network affiliates). I have attached a copy of the incident report and a copy of the notification letter that was sent out to patients.

If you have any additional questions regarding this incident please contact me via email at lizh@sihb.org or by phone at 206-324-9360, extension 1136.

Sincerely,

Elizabeth Henry,
Site Manager

Attachments (2): Incident Report
Notice to Patients

SEATTLE INDIAN HEALTH BOARD
HIPAA INCIDENT REPORT

DATE OF INCIDENT: August 10, 2016

NATURE OF INCIDENT: This incident was a hack of an end-user's email account

DETAILS OF INCIDENT: A hacker from Nigeria accessed an end-user's (Brij) email account at 6:00 AM. The hacker hijacked the user's email account and began sending a canned spam message to thousands of e-mail addresses. SIHB uses Mimecast for spam filtering. At approximately 7:00 AM IT was notified that Mimecast had blocked and purged those emails from being sent. The hacker (or the hacker's automated system) continued to send the messages, unaware that they were being blocked by Mimecast.

At approximately 10:00 AM, IT shut down SIHB's Zimbra email system to terminate the hacker's access. IT also changed all user passwords to prevent future logins by the hacker(s).

IT examined the Zimbra system logs as standard procedure to assess the nature and extent of the incident. The Zimbra logs indicate that the hacker continued in his / her attempts to send emails to individuals around the world. In our experience, this incident was representative of a typical compromised account email blasting hack.

IT then examined the "Sent" messages folder for the effected end-user. IT found no evidence that any email messages of any kind were sent or forwarded by the hacker except those that were specifically sent as part of the canned "go to this link" blasts. A last email was sent to everyone in the SIHB local distribution list telling recipients to go to a link to update their security information. This email was also blocked by Mimecast and not sent.

RISK TO PHI: The logs details do not include information specifically pertaining to emails that may have been viewed by the hacker. As such, we cannot know what the person saw in emails that were in the user's "Sent" folder or "Inbox". What we do know with certainty is that by 7:00 AM (as noted above) the hacker was prevented from sending email, and that the hacker was not aware of that fact. It is remotely possible that the hacker could have performed "screen copy" duplication of information, or that they could have otherwise downloaded the user's email information. IT cannot cannot confirm or reject that possibility outright.

REMEDIATION: The issue is 100% remediated as noted elsewhere in this report.

PROPHYLAXIS: IT is actively working on a project to move all end-users to Microsoft Office 365 email with HIPAA compliance rulesets. Further, IT has forced a password change

for every SIHB end-user as noted elsewhere herein. Lastly, IT is working to implement more structured password management and control measures.

Seattle Indian Health Board

For the Love of Native People

October 7, 2016

Hello,

I am writing to inform you that your protected health information may have been accessed by an outside party and therefore may have been breached. The Seattle Indian Health Board (SIHB) experienced a security attack to an employee email account on August 10, 2016. Access to the account lasted approximately 4 hours before the SIHB IT department shut down our email system. The information accessed may or may not have included your name, date of birth, patient ID number, social security number, along with other protected health information. The security of your data is extremely important to us at SIHB and we apologize for this incident's impact on you.

We immediately launched an in-depth investigation to evaluate the extent of this incident. We were unable to confirm whether or not any individual emails that contained protected health information were accessed externally. Our Chief Information Officer assumes that access was unlikely given the nature of the attacker's behavior while in the account. Our IT department concluded that no emails were sent or forwarded out of the account besides messages that were created by the hacker and sent to unknown recipients. While our investigation indicated the risk of exposure of patient information was low, we want to inform you of this possible exposure and reassure you that we are following all regulations under the Health Insurance Portability and Accountability Act (HIPAA).

We assure you that the proper measures have been and continue to be taken to avoid incidents like this in the future. Our IT department has forced a password change for every SIHB staff member and is working to implement more structured password management and control measures. Our IT department educated staff members about the importance of password safety. Finally, our IT staff are actively working on a project to move all staff to a more secure email system with stronger protections against today's security threats.

We understand the importance of protecting your private information and recommend you begin immediate monitoring of your bank accounts and credit reports for fraud. Report any unusual activity to your bank or credit card companies. Below is a list of the Credit Bureaus and their contact information.

Equifax	1-888-766-0008	www.equifax.com
Experian	1-888-397-3742	www.experian.com
Transunion	1-800-680-7289	www.transunion.com

If you would like more information about this matter or the protections we have in place to guard against the unauthorized access to patient information, please call (844) 518-3969. This toll-free number will be set up and available by October 12, 2016 with more details.

Again, I apologize for this incident and thank you for being a patient of Seattle Indian Health Board.

Sincerely,

Esther Lucero, MPP
Chief Executive Officer
Seattle Indian Health Board

Cc: Pt. Record