Exhibit B –

HHS OCR Breach Filing Acknowledgment (Oct 19 2023 9:43 a.m.)
Official record of the HIPAA breach report naming **Nuvem Health LLC** as Business Associate and identifying the "master key to our healthcare customers" risk. Demonstrates contemporaneous **protected disclosure** under federal law.

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Form Approved: OMB No. 0945-0001

Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

This site is available as we continuously work to make improvements to better serve the public. Should you need assistance with this site or have any questions, please email ocrprivacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697.

To file a breach report, please enter information in the wizard pages below. A field with an asterisk (*) before it is a required field.

Download Sample Form (PDF)

General | Contact | Breach | Notice of Breach and Actions Taken | Attestation | Summary

Summary: Please check the information on this page is correct and click the Submit button at the bottom to submit the breach notification.

Print

* Breach Affecting: **500 or More Individuals**

* Report Type: **Initial Breach Report**

* Are you a Business Associate filing on behalf of a Covered Entity? **Yes**

Business Associate

Completion of this section is required if the breach occurred at or by a Business Associate or if you are filing on behalf of a Covered Entity.

Name of Business Associate: **Nuvem**
Street Address Line 1: **445 Broadhollow Rd**
Street Address Line 2: **Suite 320**
City: **Melville**
State: **New York**
ZIP: **11741**

Business Associate Point of Contact Information

* First Name: **Albert** * Last Name: **Rojas**

* Email: **arojas@nuvem.com**

* Phone Number: (Include area code):

Phone Number	Usage
(646) 866-1669	Home / Cell

Enter the contact information for all Covered Entities you are filing on behalf of.

Covered Entity 1

* Name of Covered Entity: **nuvem**
* Street Address Line 1: **445 Broadhollow Rd**
Street Address Line 2: **suite 320**
* City: **Melville**
* State: **New York**

* ZIP: 11741

Business Associate Point of Contact Information

* First Name: Albert * Last Name: Rojas

* Email: arojas@nuvem.com

* Phone Number: (Include area code):

Phone Number	Usage
(646) 866-1669	Home / Cell

* Type of Covered Entity: Healthcare Provider

* Breach Start Date: 10/19/2023 * Breach End Date: 10/19/2023

* Discovery Start Date: 10/19/2023 * Discovery End Date: 10/19/2023

* Approximate Number of Individuals Affected by the Breach: 400000

* Type of Breach: Hacking/IT Incident

* Location of Breach:

Other

* Location of Breach (Other): Giving a third party administration access to our database which is the master key to our healthcare customers. The third party can do anything.

* Type of Protected Health Information Involved in Breach:

Clinical
Demographic
Financial

* Clinical

Diagnosis/Conditions
Lab Results
Medications
Other Treatment Information

* Demographic

Address/ZIP
Date of Birth
Drivers License
Name
SSN

* Financial

Claims Information

* Brief Description of the Breach: Please see point F below "It should also have a sysadmin login in each monitored SQL Server instance." _____ info@madeiradata.com I www.madeiradata.com I +972-9-7400101 1. General We use SolarWinds SQL Sentry as the main tool to collect performance data from your servers. We chose SentryOne because we believe this is the most comprehensive and advanced tool for monitoring SQL Server. At the same time, this tool is also very lightweight, so it has a low impact on your servers. 2. What We Need from You To set up the collection tools successfully, we would like to ask you to prepare a few things in advance. a. We recommend installing SQL Sentry on a separate machine, which will serve as the monitoring server. b. If you prefer not to use a separate machine, then we can also install it on one of the production servers (one of the SQL Server instances we are about to review). This is less recommended, simply because we prefer to make

changes to your production servers as little as possible, and reduce "observer effect". c. Here are the minimum requirements for the monitoring server: • CPU – 8 cores • RAM – 8GB • Free Disk Space – 50GB • Windows Server 2012 / Windows 10 or higher • SQL Server 2016 SP1 Standard Edition (Developer or Evaluation Editions are also fine, and it's free) d. If possible, create a dedicated domain account to be used by the SQL Sentry monitoring service. e. If your servers are not in a domain, then create a dedicated local account on the monitoring server and on each one of the monitored servers. All accounts should have the same username and password. f. The account should have Windows admin privileges on the monitoring server and all monitored servers. It should also have a sysadmin login in each monitored SQL Server instance. g. Make sure that the monitoring server can access the monitored servers through the network and connect to the monitored SQL Server instances. h. Make sure that the monitoring server can access the internet to download the SQL Sentry trial version. This internet access can be temporary, just for the installation, and it can be blocked as soon as the installation is completed successfully. Alternatively, we can download the installation media to a separate server, which has access to the internet, and then copy the media to the monitoring server. 3. Remote Connection (Optional) To allow us to do a better job, we ask you to grant us a remote connection to the monitoring server and the monitored servers. We require a VPN connection (according to your security policies) and an RDP connection to each one of the servers

* Safeguards in Place Prior to Breach:

None
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: **10/19/2023**

Individual Notice Provided Projected/Expected End Date: **10/19/2023**

Was Substitute Notice Required? **No**

Was Media Notice Required? **No**

* Actions Taken in Response to Breach:

Other

* Describe Other Actions Taken: **Nothing was taken. Team has been alerted but nothing is happening**

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

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

* Name: **Albert Rojas** Date: *10/19/2023*

Please review the information on this page for accuracy. When finished, please select the "Submit This Breach Notification" button at the bottom to submit the 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.

Submit This Breach Notification

← Back

If you have questions or would like to provide feedback about the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification process, or OCR's investigative process, please send us an email at OCRbreachreportingfeedback@hhs.gov.