OFFICE OF THE DIRECTOR

Tina Kotek, Governor

500 Summer St. NE E-20
Salem, OR 97301
Voice: 503-947-2340
Fax: 503-947-2341
www.oregon.gov/oha

September 21, 2023

Senator Aaron Woods, Co-Chair
Representative Nancy Nathanson, Co-Chair
Joint Legislative Committee on Information Management and Technology (JLCIMT)
900 Court St. NE
Salem, OR 97301

SUBJECT: Written Testimony on the PH Tech Third Party MOVEit Data Breach

Dear Co-Chairs and Members of the Committee:

Per your request, Oregon Health Authority (OHA) is providing written testimony on the PH Tech third party MOVEit data breach that impacted approximately 1.7 million Oregon Health Plan (OHP) members data.

Background

On June 2, 2023, PH Tech was notified that Progress MOVEit, a vendor who supports the secure transfer of electronic files, had a vulnerability that could allow attackers to access the MOVEit system and potentially download files. Upon learning this, PH Tech took immediate action to move the system offline and launched an investigation to determine whether PH Tech systems were affected. PH Tech also engaged a forensic cybersecurity firm to assist in the investigation and notified the Federal Bureau of Investigation (FBI).

From the investigation, it was discovered and validated that the Progress MOVEit's software was exploited by an unknown actor and that PH Tech data files were downloaded without authorization. PH Tech determined that data it holds for some of its customers had been affected by this event on June 16, 2023, and notified those customers the same day. The compromise occurred on May 30, 2023.

- On August 2, 2023, PH Tech, announced publicly a data breach, in which attackers accessed approximately 1.7 million OHP members' data.

- PH Tech is a private vendor that provides services to some Coordinated Care Organizations (CCOs) that utilize OHP member data with health care plans, helping with things like customer service, enrollment, and payment services.

- This third party data breach did **not** involve or compromise state systems.

- Due to the OHP member data involved, OHA was engaged and monitoring the responses between CCOs and PH Tech from the time OHA was notified on June 22, 2023.

Notifications

Personal information and protected health information was compromised from a variety of files including enrollment, authorization, and claims files. No member specific financial information was included in this data.

- On Monday July 31, PH Tech began sending out the data breach notification letters via mail to impacted OHP members with information, and instructions on how to activate free credit monitoring. The notifications letters were translated into 12 different languages.

- On July 24, Dave Baden, OHA's interim director, called on PH Tech and CCOs to notify OHP members promptly and to ensure that OHP members received information that was understandable and appropriately translated. State officials urged OHP members to read the notifications they'll receive from PH Tech and take steps to protect their credit. Due to the extreme impact of this third-party data breach to OHP members, Dave Baden called upon OHA staff to support CCOs in an advisory and consulting capacity throughout the course of the third-party data breach with PH Tech.

Regulatory and Contractual Relationships

This was not a breach of State systems. PH Tech is a private vendor subcontracted by some CCOs for services that utilize OHP member data. Since the data breach took place in PH Tech's IT systems, from a state and federal regulatory perspective, PH Tech is the company responsible for reporting and notification of the data breach.

- OHA does not have a direct contractual relationship or regulatory oversight over PH Tech. CCOs hold executed contracts with PH Tech.

- OHA has CCO contracts for OHP services paid with Medicaid funds with 12 different companies. Two of these companies serve multiple non-contiguous regions, and each region is covered by a separate contract. As a result, there are 16 separate Medicaid contracts held by 12 companies. Additionally, each Medicaid contract has a corresponding non-Medicaid contract, which is for OHP services paid only with state funds. The Medicaid and non-Medicaid CCO contracts are nearly identical but must be separate due to federal Medicaid requirements. In 2023, the non-Medicaid contract covers the majority of OHP services for Healthier Oregon Program members as well as all services for the COFA and Veterans dental-only programs. As a result, there are 32 separate CCO contracts held by 12 different companies.

  o Ten of the 12 companies with CCO contracts for calendar year 2023 were affected by the PH Tech breach.

  o The contracts for calendar year 2023 require CCOs to report security/privacy incidents to OHA within 5 business days of discovery. OHA has revised this language for calendar year 2024 to require such reporting within one 1 business day. The CCO is responsible for ensuring that all applicable OHA contract requirements, including this reporting timeframe, are included in its subcontracts.

    ▪ In a memo dated August 31, 2023, OHA requested that CCOs implement the one business day timeframe for the remainder of 2023. However, this

action is at the discretion of the CCO whether they do so before it is required in 2024.
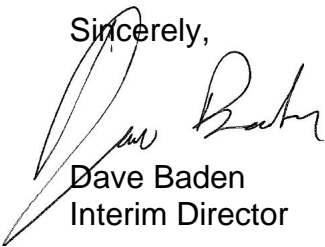
Timeline

PH Tech immediately disabled platform access, patched the vulnerability, and rebuilt internal access to the PH Tech platform to prevent further unauthorized access of files through the Progress MOVEit software.

- June 16 - Per PH Tech, they began notifying their customers, including CCOs, that they had experienced a data breach.

- June 22 - PH Tech notified OHA as a courtesy, due to the agency's concern for OHP members.

- July 25 - PH Tech told state officials it conducted extensive forensic analysis through July 25th. This analysis identified the individuals who were impacted, so they could be notified.

- July 31 - PH Tech began mailing letters with more information and resources to those impacted.

- August 2 - PH Tech announced publicly a data breach, in which attackers accessed approximately 1.7 million OHP members' data.

As custodians of the data, PH Tech will have more details about the specifics of the breach. Answers about specifics of the breach can be obtained by emailing: media@phtech.com.

Thank you for your interest in this important matter.

Sincerely,

Dave Baden
Interim Director