STATE OF OKLAHOMA
CYBER COMMAND

Mark Gower
State of Oklahoma Chief Information Security Officer
and Cyber Command Director
3115 N. Lincoln Blvd.
Oklahoma City, OK 73105

August 09, 2018

General Doug Elliot
Executive Director
Oklahoma Department of Veterans Affairs
2311 N. Central
Oklahoma City, OK 73105

General Elliot,

Thank you, sir for contacting the Office of Management and Enterprise Services, State Chief Information Security Office. Your request to investigate for a potential HIPAA violation or data breach has been received and processed. Investigative staff from OMES reviewed the issue with Oklahoma Department of Veterans Affairs (ODVA) staff and the Electronic Medical Record (EMR) vendor system PointClickCare. The following report is the conclusion of that review.

Incident Description: On July 25th the Office of Management and Enterprise Services was overseeing telecommunications maintenance on the state fiber, for a scheduled outage. This outage had an unintended impact on two ODVA locations (Norman and Lawton). The ODVA sites contacted the appropriate ODVA informatics team, who reviewed the outage and the need for care, and made the authorization to enable the ability in the PointClickCare system to allow for mobile access for limited individuals, during the timeframe of the network outage.

Findings: The end result of the findings does not show there to be any identified issues with violations of the HIPAA Privacy or Security Rules, or the State of Oklahoma Breach Notification Act. This determination was made based on the following factors:

- Access to the EMR from mobile devices was authorized on a limited basis to address an emergency need, for the treatment of patients in care. This access was performed by vetted and authorized ODVA staff who have access to ePHI and PII in their normal course of duties and are required to maintain compliance to ODVA HIPAA privacy and security training, policies and procedures. These vetted staff have access to this same sensitive data on a daily basis and are trained to appropriately handle and process that data in a secure manner with the privacy controls that are mandated in the HIPAA Privacy Rule.
- The EMR was accessed by a limited number of authorized ODVA staff through the use of mobile devices which still required the use of mandated security credentials and processes that are prescribed in the HIPAA Security Rule and supported by the EMR vendor to provide mobile access securely.

- The EMR provides the required authentication for every user and establishes encrypted communications between a device and the EMR to keep data in transit secure as required by the HIPAA Security Rule.
- The EMR does not store a local copy of data on the device when it is accessed and it does not cache data on the device, meeting security requirements.
- The EMR provides a secure mobile device module for access to records as part of the core EMR system. This is an approved, secure method of accessing the EMR.

This report concludes our review of this matter. I recommended that you continue your collaboration between the US Department of Health and Human Services, Office of Civil Rights to follow on to your original self-reporting to them of the this matter to include this report and its findings. My office will be available to support the ODVA if any further questions are required. I commend you for your diligence and support in reporting your concerns.

Sincerely,

Mark Gower, C|CISO, CISSP, CISM, CBCP
State of Oklahoma Chief Information Security Officer and
Cyber Command Director