HITRUST

Letter of Certification

August 7, 2018

TigerText
2110 Broadway
Santa Monica, CA 90404

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CSF Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST CSF Assurance Program, the following business system and infrastructure of the organization meet the HITRUST CSF v9 Certification Criteria:

TigerText - TigerConnect and the corresponding TigerConnect Infrastructure

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time
- No data security breach reportable to a federal or state agency by law or regulation has occurred
- No significant changes in the business or security policies, practices, controls and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria
- Annual progress is being made on areas identified in the Corrective Action Plan (CAP)
- Timely completion of the interim review as defined in the HITRUST CSF Assurance Program Requirements

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information security tailored to the healthcare industry. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the organization must have a CAP that outlines its plans for meeting such requirements.

HITRUST performs a quality assurance review consistent with the HITRUST CSF assurance program requirements to ensure that the scores are consistent with the testing performed by the HITRUST CSF Assessor organization. The controls required for HITRUST CSF certification were also aggregated, scored and mapped to the NIST Cyber Framework requirements.

A full copy of the certification report has also been issued to the organization listed above. This full report includes additional details on the scope of the assessment, a representation letter from management, testing results for those controls required for certification, a benchmark report comparing the organization's results to industry results, details on CAPs required for

certification, as well as the NIST CsF mapping and the completed questionnaire. If interested in obtaining a copy of the full report, you will need to contact the organization directly.

Additional information on the HITRUST CSF Certification program can be found at the HITRUST website: www.hitrustalliance.net.

HITRUST