Quality Assessment and Accountability Systems

CASAS Statement Regarding Privacy and Confidentiality

CASAS manages student-level data that comprises personal (private) information in compliance with all applicable federal and California state privacy laws including, but not limited to, the FERPA of 1984 (20 U.S.C. Sec 1232g), HIPAA, COPPA, California Education Code sections 49060 to 49070, and California Assembly Bill 1584. CASAS security measures incorporate advanced industry standards and protocols to ensure data is secure and confidential and that unauthorized personnel are unable to gain access to personal data.

Specifically, CASAS ensures compliance with all of the provisions listed below.

A. For purposes of this Statement, the following terms have the following meanings:

(1) "Learner" means a person who provides personally identifiable information to an end-user that is subsequently stored in the CASAS software database.

(2) "End-user" includes school districts, community colleges, workforce agencies, other state and local governmental agencies, non-governmental/community-based organizations, and private corporations.

(3) (A) "Learner records" means any information directly related to a learner that is maintained by the end-user.

(3) (B) "Learner records" does not mean any deidentified information, including aggregated deidentified information, used by CASAS to improve its software applications and better inform end-users of new features related to adaptive or customizing learning.

(4) "CASAS" refers to the provider of TOPSpro Enterprise, CASAS eTests and NEDP digital assessment software or services, including cloud-based services, for the digital storage, management, and retrieval of learner assessment and accountability records.

B. The online environment in which CASAS hosts its software applications – TOPSpro Enterprise, CASAS eTests, NEDP, and WLNAS – has received Federal Information Security Management Act (FISMA) Moderate Authorization and Accreditation from the U.S. General Services Administration. FISMA requires federal agencies to develop, document, and

implement an information security system for its data and infrastructure. The security and compliance framework covers FISMA Low and Moderate, PCI DSS Level 1, FIPS 140-2, ISO 27001, and SAS-70 type II. The server environment additionally complies with HIPAA regulations and is subject to third party audits.

By accessing CASAS online software applications end-users enter into a contract/online account agreement (OAA) with CASAS for either or both of the following purposes:

(1) To obtain services, including cloud-based services, for the digital reporting, management, and retrieval of learner records.

(2) To obtain digital educational software that authorizes CASAS to access, store, and use learner records in accordance with the contractual provisions listed in subdivision **C**.

C. CASAS assures such end-users that establishing an online account for purposes of subdivision **B** that it will maintain the continued confidentiality and security of the student data processed, stored, or transmitted under the OAA. End-users shall also establish a system of safeguards that will at minimum include the following:

(1) Procedures and systems that ensure all learner records are kept in secured facilities and access to such records is limited to personnel with legitimate interests who are authorized to have access to said data.

(2) All designated CASAS and end-user staff involved in the handling, transmittal, and/or processing of data recorded under the OAA will be required to execute a confidentiality agreement requiring said personnel to maintain the confidentiality of all learner related personally identifiable information.

(3) Procedures and systems that shall require the use of secured passwords to access computer databases used to process, store, or transmit data provided under this OAA.

(4) Procedures and systems, such as good practices for assigning passwords, shall be developed and implemented to maintain the integrity of the systems used to secure computer databases used to process, store, or transmit data provided under the OAA.

(5) Procedures and systems that ensure that all confidential learner data processed, stored and/or transmitted under the provisions of the OAA shall be maintained in a secure manner that prevents the interception, diversion, or other unauthorized access to said data. No data will be submitted or accepted unless it is processed through the secure, encrypted upload steps or through a secure FTP site.

(6) Secure procedures to return submitted custom data to end-users that require revision and/or submission will be used. This process will ensure data are securely transferred and valid data are available through the Transitions Data initiative.

(7) The procedures and systems developed and implemented to process, store, or transmit data provided under the OAA shall ensure that any and all disclosures of confidential learner data comply with all provisions of state and federal law relating to the privacy rights of learners including, but not limited to, the FERPA of 1984 (20 U.S.C. Sec 1232g), HIPAA, COPPA, California Education Code sections 49060 to 49070, and California Assembly Bill 1584.