 iKeepSafe

## Introduction

The iKeepSafe Privacy Program is available to operators and service providers of websites and online services, data management systems and other technologies that are, in whole or in part, intended for use in and by schools, and which may collect, store, process or otherwise handle student data.

This *iKeepProfile* is intended to assist you in determining whether Multi Health Systems ("**MHS**") complies with FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that Multi Health Systems has been assessed for alignment with the iKeepSafe FERPA and California Privacy Program Guidelines.

## Product Overview

MHS: [www.mhs.com](www.mhs.com)

Multi Health Systems Inc. (MHS) serves clients in educational, clinical, corporate, public safety, government, military, pharmaceutical, and research settings. The Assessments are used in a wide range of critical decision-making processes. The clinical tools are trusted to inform psychological diagnoses that can impact prescribed medication, therapy, or treatment programs for children and adults.

.

 iKeepSafe

# Agreement

As related to the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g), MHS agrees:

1. Student records obtained by MHS from an educational institution continue to be the property of and under the control of the educational institution. The educational institution retains full ownership rights to the personal information and education records it provides to MHS.
2. MHS does not collect or store any student-generated content. In the event the platform is updated to incorporate such a feature, MHS will amend this statement to describe the means by which students may retain possession and control of student-generated content.
3. MHS will not use any information in a student record for any purpose other than those required or specifically permitted by the MHS Terms and Conditions and Privacy Policy.
4. Parents, legal guardians, or eligible students may review personally identifiable information in the student's records and correct erroneous information by contacting their educational institution.
5. MHS is committed to maintaining the security and confidentiality of student records. Towards this end, we take the following actions:
   a. we limit employee access to student data to only those employees with a need to such access to fulfill their job responsibilities;
   b. we conduct background checks on our employees that may have access to student data;
   c. we conduct regular employee privacy and data security training and education; and
   d. we protect personal information with technical, contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.
6. In the event of an unauthorized disclosure of a student's records, MHS will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. MHS will delete or de-identify personal information when it is no longer needed, upon expiration or termination of our agreement with an educational institution with any deletion or de-identification to be completed according to the terms of our agreement with the educational institution, or at the direction or request of the educational institution.
8. MHS agrees to work with educational institution to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians or eligible students with the ability to inspect and review student records and to correct any inaccuracies therein as described above.
9. MHS prohibits using personally identifiable information in student records to engage in targeted advertising.
10. MHS will not make material changes to our Terms of Use or Privacy Policy, including making significant changes impacting the collection, use, disclosure or retention of data collected without prior notice to the educational user.

As related to the Student Online Personal Information Protection Act (SB 1177 - "SOPIPA"), MHS agrees:

Prohibitions:

1.  MHS does not target advertising via the MHS service or on any other website using information about a K-12 student, their families/guardians or educators acquired from a use of the technology.

2.  MHS does not use information, including persistent unique identifiers, created or gathered by the MHS service to amass a profile about a K–12 student, their families/guardians or educators except in furtherance of K–12 school purposes.

3.  MHS does not and will not sell, rent, or otherwise provide personally identifiable information to any third party for monetary gain.

4.  MHS does not disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Obligations:

5.  MHS is committed to maintaining the security and confidentiality of pupil records as noted herein.

6.  MHS will delete student information when requested by school district.

7.  MHS will disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

## Third Parties

MHS does not sell, trade, lease or loan the personal information they collect or maintain, in the course of providing the service, to any third party for any reason, including direct marketers, advertisers, or data brokers.

MHS contracts with other third-party companies to perform business functions or services on their behalf but does not share any PII with these third parties. MHS has agreements in place with third parties to deliver the authorized service and to ensure they maintain the confidentiality and security of the information. The agreements align with MHS data privacy and security policies and expectations.

MHS will make available the list of third-party service providers upon request.

## Product Data List

| | Data Collected for Operation: | General Purpose of Data Collection |
|---|---|---|
| 1 | Student First and Last Name | Required to support product functionality |
| 2 | Student Email Address | Required to support product functionality |
| 3 | Student Password | Required to support product functionality |
| 4 | Teacher First and Last Name | Required to support product functionality |
| 5 | Student Age/DOB | Required to support product functionality |
| 6 | Student Gender | Required to support product functionality |
| 7 | Parent first and last name | Required to support product functionality |
| 8 | Parent physical address | Required to support product functionality |
| 9 | School Name | Required to support product functionality |
| 10 | ACCESS TIME | Business Intelligence |
| 11 | Time Spent on Site | Business Intelligence |
| 12 | Referring URLs | Business Intelligence (Browser) |
| 13 | PAGE VIEWS | Business Intelligence (Browser) |
| 14 | IP Address | Business Intelligence |

## Data Review Process

MHS provides users direct access to their personally identifiable information via product functionality. Any other request for access to personally identifiable information held by MHS must be made via the following:

privacyofficer@mhs.com

USA: 1-800-456-3003
CDA: 1-800-268-6011
INTL: +1-416-492-2627

416-492-3343

# Security Protocols

MHS has a comprehensive Security Program in place designed to protect the confidentiality, integrity and availability of systems, networks and data. The following is a general overview of data security protocols:

### Data in Transit
Data is transferred using HTTPS.

### Data at Rest
MHS utilizes MICROSOFT services (BitLocker, ATP) for ensuring the security of data residing on laptops/pcs. Production databases are fully encrypted at rest, using AES256 level encryption.

### Data Center Security
Client data, as well as back the backup data are stored in the United States at Rackspace's data center locations.

### Personnel

Background Checks: All employees with access to student data have undergone background checks.

Training: Employees of MHS receive annual privacy and security training that includes FERPA.

Access: Access to student data is role-based; limited to those employees who need access to perform job responsibilities. Employees are given access to the minimum services that are required for their job function.

## Data Retention and Deletion

Users may deactivate their account at any time by accessing their account through the MHS platform.

Following the termination of a license, a school or district may request that MHS deactivate and de-identify Student Information and MHS will do so, unless the school, district, or applicable regulations require the retention of such data, in which case the records shall be de-identified upon the expiration of the retention period.

## California Consumer Privacy Act (CCPA)
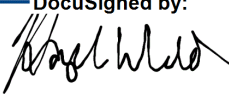
Users may request disclosure of personal information held by MHS. Users may also request the deletion of personal information. MHS does not sell Personal Information in accordance with CCPA.   Users will also be notified if personal information will be collected beyond the terms of the privacy policy and how that information will be used.

# Accuracy Statement

MHS hereby confirms the accuracy and truthfulness of all information contained in the MHS product profile and has authorized iKeepSafe to make the profile available to any interested schools.

DocuSigned by:

DBD2DF482BEA458...

(Signature)

Hazel Wheldon
CEO
MHS, Inc

MHS  service has been reviewed and found in alignment with iKeepSafe's FERPA and California Privacy Program Guidelines as indicated by this product profile. MHS has been awarded the iKeepSafe FERPA and California Privacy Program badges.

DocuSigned by:

Amber Lindsay

4936610B3823488...

(Signature)

Amber Lindsey
President & CEO
iKeepSafe

01/10/2020

## Copyright