iKeepSafe Product Profile
eCare Vault, Inc.

Introduction

The iKeepSafe California 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 the eCare Vault Service complies with FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that the eCare Vault Service has been assessed for alignment with the iKeepSafe California Privacy Program Guidelines.

The *iKeepProfile* is not legal guidance, nor does it guarantee or otherwise assure compliance with any federal or state laws. If you have questions on how to use the *iKeepProfile* to support your school's compliance efforts, please contact your school attorney.[1]

Product Overview

eCare Vault: https://ecarevault.com/

eCare Vault provides a unique SOC 2 Type II, HIPAA and FERPA-compliant SaaS platform at the intersection of the Education, Community Care and Public Safety sectors that acts as a secure, privacy-compliant care team collaboration bridge between departments of child and family services, school districts, law enforcement entities, special education and health service providers, parents, and community services.

The eCare Support Hub is a modular, ready-to-deploy, workflow management solution with a trauma-informed lens. Our person-centered hub engages and supports children, youth & families along their entire care journey in ways that ensure equitable access to personalized resources and timely services while ensuring policy compliance.

The solution's flexible, human-centered, collaboration and event-based workflow design enable users to coordinate, capture, and report upon services and interventions, drive and track the stages of closed-loop referral management, track the longitudinal outcomes and needs of clients, and gain insight into data to be able to display effectiveness of programs through short- and long- term analytics.

eCare Vault's specific capabilities include:

- Customized dashboards and reports on client services, supports, and interventions that can

be filtered and downloadable;

- Granular, permission-based access controls and privacy compliance to ensure that only those who require access to certain data and information can see it, while still enabling seamless sharing of information between users, within a SOC 2-and HIPAA-compliant environment;
- Dynamic, client-centered teams for those identified with support needs, comprised of relevant stakeholders for cross-department and cross-county communication and coordination;
- Individual client-centered dashboards for an integrated view into the status of services, referrals, and placements, along with historical data and recommended next steps;
- Service Notes to enable a one-step process to track and log comprehensive notes around administered services, interventions, and assessments for clients all in one place;
- Forms to digitize manual, burdensome administrative processes with automated event-based alerts and notifications to ensure actions are taken, such as internal referral processes;
- Document Management to upload, share, and store screens, assessment, records, and documents relevant to individual students, to facilitate seamless access to information as;
- Multi-way, threaded discussions to allow team members to share relevant contextual information and observations on student cases and provide recommendations; and
- The ability to invite external community members to join a client's support team as appropriate, to improve coordination with community agencies.

eCare Vault's solution is currently utilized across all 50 states, District of Columbia, and Puerto Rico - by government, community care agencies, Medicaid eligibility offices, regional service centers, and educational institutions.

A unique person-centered SaaS solution, eCare Vault's flexible workflow-driven features are differentiated from any other marketplace options.

Agreement

A. As related to the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g) and California AB 1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1), eCare Vault agrees:

1. Pupil records uploaded to the eCare Vault service by an Educational Representative continue to be the property of and under control of that Educational Representative. eCare Vault does not directly touch any information nor have routine access to the data and recognizes that any information exchanged is the property of the Educational Representative.

2. Authorized users may retain possession and control of their own generated content by signing into the eCare Vault Service and downloading any information that they have uploaded onto the eCare Vault platform.

3. It shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the Terms of Service and Privacy Policy for the eCare Vault Service.

4. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information by contacting their Educational Representative. If they are a Team Member, they can access, update and delete data through signing into their account.

5. It is committed to maintaining the security and confidentiality of pupil records. To that end, eCare Vault has taken the following actions: (a) limiting employee access to student data based on roles and responsibilities; (b) conducting background checks on employees who have access to student data; (c) conducting privacy training that includes FERPA for employees with access to pupil data; (d) protecting personal information with technical, contractual, administrative, and physical security safeguards in order to protect it from unauthorized access, release or use.

6. In the event of an unauthorized disclosure of a pupil's records, eCare Vault will promptly (within 20 days of becoming aware of the issue) notify the Educational Representative. The notification will include: date of the breach, the types of information that were subject to the breach; general description of what occurred; steps eCare Vault is taking to address the breach; the person at eCare Vault whom the data holder can contact regarding questions about the breach. eCare Vault will keep the authorized user fully informed until the incident is resolved.

7. It will delete personally identifiable data upon request of the Educational Representative and/or upon expiration of the services agreement. See Security Protocol section.

8. It agrees to work with the Educational Representative 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 pupil records and to correct any inaccuracies therein as described in statement 4 above.

9. It prohibits using personally identifiable information in pupil records to engage in targeted advertising.

10. It will not make material changes to its privacy and security policies, including adding practices around new or additional data collection, or changes that may lessen the previously noted protections without prior notice to the Educational Representative, separate from any notice in a "click wrap" agreement.

B. As related to Student Online Personal Information Protection Act (SB 1177 -"SOPIPA"), eCare Vault agrees:

Prohibitions:

1. eCare Vault does not target advertising via the eCare Vault Service or on any other website using information about a K-12 student acquired from a use of the technology.

2. eCare Vault does not use information, including persistent unique identifiers, created or gathered by the eCare Vault Service to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

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

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

Obligations:

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

6. eCare Vault will delete district-controlled student information when requested by that school district.

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

Security Protocols

eCare Vault has a comprehensive Information Security Program in place that ensures the confidentiality, integrity and availability of systems, networks and data. The following is a general overview of data security protocols:

Data In Transit
Uploads are by HTTPS. Data is encrypted during transmission.   All documents uploaded to the eCare Vault Service are encrypted during transmission between the Client (typically a browser web client on the user's computer) and the Service via the standard SSL Protocol.

Data at Rest
Documents are encrypted upon receipt by the eCare Vault Server. The encrypted documents are stored in Amazon's S3 (Simple Storage Service). When a document is shared by one user (sender) to be viewed by another user (recipient), the document is only briefly decrypted by the server (in memory) in order to make a copy.
In the future, we will look to use a similar offering by Microsoft Azure (Azure Blob Storage) to facilitate encrypted document storage.

Data Storage
Data is stored in a RDS database (housed in AWS), which is encrypted. Data is also stored in Amazon's S3. All users specific data in S3 is encrypted and potential PII/PHI (e.g. documents and photos uploaded by the user, discussions, etc.) is encrypted with the users public key so that it can be decrypted only when their private key is protected with a user-specific password. Data backup occurs through automatic snapshots stored in Amazon's S3 servers. All

4

backups are encrypted. In the future, we will look to use Microsoft Azure's hosted database solution to securely store encrypted data.

Data Center Security

eCare Vault utilizes data centers operated by Amazon Web Services (AWS) and by Microsoft Azure.Both vendors have extensive experience in designing, construction, and operation large-scale data centers. Microsoft Azure and AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at the building ingress points by professional security staff utilizing video surveillance, intrusion detection system and other electronic means. Authorized staff must pass a two-factor authentication a minimum of two times to access data center floors. Microsoft Azure and AWS only provide data center access and information to employees and contracts who have a legitimate business need.

Personnel

Training: eCare Vault conducts privacy and security training for all employees.

Access: Access to student data is role-based; limited to those employees who need access to perform job responsibilities. All employees with access to PII/PHI have undergone background checks.

Policy: eCare Vault has created and maintains HIPAA Privacy and Security Policies.

Data Deletion

eCare Vault will delta personally identifiable data, expect the profile information of the authorized user and care recipient(s) to ensure accurate record keeping, upon request of the Educational Representative and/or upon expiration of the services agreement as per the process specified below:

Data deletion practices when Authorized user exits a Care Team:

Prior to exiting the team, the authorized user has the opportunity to download any information that they have uploaded and/or received prior to exiting the team. Once an authorized user exits a team, all data that was uploaded and/or received by the authorized user for that team will be deleted from the authorized user's account. Any information that has been previously shared by the authorized user prior to exiting the team cannot be unshared. Note: Prior to exiting a Team, an authorized user must transfer ownership of the care teams for which they are a team owner. If ownership is not transferred, the care team is "frozen" and remaining team members can no longer collaborate on the related care recipient.

Data deletion practices when Authorized user Terminates account:

Prior to terminating the account, the authorized user has the opportunity to download any information that they have uploaded and/or received across all of the care teams they are a part of. If the authorized user does not transfer ownership prior to termination of their account, all teams in the terminated account for which the authorized user is a team owner will be frozen. Any information that has been previously shared by the authorized user prior to exiting the team cannot be unshared.   eCare Vault may keep deidentified and aggregated data for Analytics.

5

Third Parties

eCare Vault 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.

eCare Vault contracts with other third party companies to perform business functions or services on their behalf and may share PII with such third parties as required to perform their functions. eCare Vault has agreements in place with all third parties with access to student personal information to ensure they only use the information for purposes necessary to deliver the authorized service and to ensure they maintain the confidentiality and security of the information. eCare Vault utilizes the following third party vendors as indicated below

Third Party	Business function or Service
MS Azure	Cloud hosting Platform
DataDog	Infrastructure Monitoring; only de-identified non-PII data
GoDaddy.com	SSL certificate provider, DNS Provider
Google Analytics	Used to monitor the performance of the service internally. No private data disclosed.
Azure EntraID B2C	Industry-standard authentication service. User emails and encrypted passwords are stored and authenticated via Azure.
Jeavio	Software engineers responsible for developing and maintaining the eCare Vault platform
Microsoft Azure	Cloud Hosting Platform
Mongo	Database for Analytics Module; only de-identified non-PII data

6

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 Age/DOB	Required to support product functionality
3	Student Gender	Required to support product functionality
4	Student State ID	Required to support product functionality
5	Parent First and Last Name	Required to support product functionality
6	Parent Physical Address	Required to support product functionality
7	Parent Phone/Mobile Number	Required to support product functionality
8	Parent Email Address	Required to support product functionality
9	Parent Password	Required to support product functionality
10	Parent Password Hint	Required to support product functionality
11	Parent Age/DOB	Required to support product functionality
12	Photograph (user generated)	Required to support product functionality ; uploaded and utilized by Care Team
13	Access Time	Business Intelligence
14	Time Spent on Site	Business Intelligence
15	Page Views	Business Intelligence
16	Referring URLS	Business Intelligence

7

Accuracy Statement

eCare Vault, Inc. hereby confirms the accuracy and truthfulness of all information contained in the eCare Vault Service profile, and has authorized iKeepSafe to make the profile available to any interested schools.

Signed and agreed:

/s/ Dan Ghammachi
(Signature)

Dan Ghammachi
CEO
eCare Vault

12/10/2024

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

DocuSigned by:

Amber Lindsay

4936610B3823488...
(Signature)

Amber Lindsay
President & CEO
iKeepSafe

12/09/2024

Copyright

© 2016 Internet Keep Safe Coalition (iKeepSafe). All rights reserved. iKeepSafe's California Privacy Assessment Program™ materials have been developed, copyrighted, and
distributed for incidental, classroom use only. iKeepSafe's copyright notice and distribution restrictions must be included on all reproductions whether in electronic or hard copy form. These materials are intended to convey general information only and not to provide legal advice or any other type of professional opinion.

Disclaimer

[1]By using the California Privacy Assessment Program or accepting any materials related to the California Assessment Program, you expressly acknowledge and agree that neither Internet Keep Safe Coalition, their affiliates, subsidiaries, or designees nor each of their respective officers, directors, employees or agents (collectively, Associates), can guarantee, certify or ensure that you are in compliance with FERPA, SOPIPA, California AB 1584, or any other state or federal laws. You understand that the California Privacy Program does not constitute legal or any other type of professional advice and the California Privacy Seal is not a legal determination.

You further acknowledge that the California Privacy Assessment Program is not officially recognized by the U.S. Department of Education or any other legislative or regulatory body, and the program does not provide any legal safe harbor. You are encouraged to consult with your attorney. Under no circumstances shall the Internet Keep Safe Coalition, or their Associates be liable for any direct, indirect, incidental, special or consequential damages that result from you not being in compliance with FERPA, SOPIPA, California AB 1584, or for any claim that you are not in compliance with these and other applicable laws. You acknowledge and represent that it is your sole responsibility to evaluate whether or not you are in compliance with these and other laws.