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 is a software vendor that provides a HIPAA-compliant, cloud-based platform for care coordination, the eCare Vault Service (Service). The Service enables parents, caregivers, teachers and health care providers to engage in seamless, organized and efficient care coordination across institutional boundaries in ways that enhance health and learning outcomes, while saving time and resources, and strengthening parent-provider partnerships.

eCare Vault's initial focus is on care coordination for children with extra developmental needs. Parents invite the child's team members to the Service and can selectively share documents, photos and engage in discussions in organized topic threads. The Service can also be used to coordinate care for adults, including elderly parents and other loved ones for whom care coordination across multiple providers is vitally important.

eCare Vault's care coordination is centered on a concept of a Care Team built around a Care Recipient - the child or adult receiving health and/or education services. The Care Team is a collection of authorized users (registered users of the service) that have been specifically invited as Team Members to receive and share health and education-related information about a specific Care Recipient. Team Members can include parents/caregivers, individual teachers, learning specialists, and health care providers who can exchange information with others via a Care Team, based on appropriate consents obtained outside the eCare Vault platform. Multiple Care Teams can be managed from a central dashboard.

There are two primary roles within the Care Team:

1. Team Owner: an authorized user and Team Member of a Care Team who has the authority to invite a Team Member, approve/decline a suggested Team Member and transfer ownership of that Care Team to another Team Member or to “freeze” the Care Team whereby they can no longer collaborate on the Care Recipient.

2. Team Member: an authorized user who has become a member of a Care Team by accepting an invitation to join that Team. A Team Member can invite another person to join the Team, or suggest to the Team Owner that a person be invited to join the Team. A Team Member can share information with other Team Members through the Service, including documents, discussions and photos.

The eCare Vault Service is a cloud-based platform that enables authorized users to build Care Teams to coordinate care around a Care Recipient - a child or adult receiving care in the form of health and/or education services. All authorized users are solely responsible for providing or obtaining all necessary authorizations and consents from the Care Recipient or parents/ guardians of a Care Recipient if the Care Recipient is a minor. Authorized users who are representatives of a school or local education agency are recognized as Educational Representatives for the purposes of complying with the student data privacy laws included herein.

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, the 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 use 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 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 HTPPS. 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 Server 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.

Data Storage

Data is stored in a RDS database (housed in AWS), which is encrypted. Data is also stored in Amazon's S3. All user 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 user's public key so that it can be decrypted only with their private key which is protected with a user-specified password

Data backup occurs through automatic snapshots stored in Amazon's S3 servers. All backups are encrypted.

Data Center Security

eCare Vault utilizes data centers operated by Amazon Web Services (AWS) who have extensive experience in designing, constructing, and operating large-scale data centers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. AWS only provides data center access and information to employees and contractors 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 delete personally identifiable data, except 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 terminating account, all the 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.

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
Jeavio	Software engineers responsible for developing and maintaining the eCare Vault platform
Amazon Web Services (AWS)	Cloud storage provider
Google	Email and document management provider
Mere Agency	Website creation, Word Press hosting
GoDaddy.com	SSL certificate provider
East Coast Catalyst	UI/UX Design
Boston Human Factors	UX Research/Design
Stratum Security	Technical penetration testing

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

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:

DocuSigned by:
Aparna Rao
CFFA7B3841094F4...
(Signature)

Aparna Rao
(Printed Name)

President & CEO
(Title)

eCare Vault , Inc.

05/10/17

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:
Holly Hawkins
B0E6FFA00A18442...
(Signature)

Holly Hawkins
President & CEO
iKeepSafe

05/10/17

Copyright

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.