# Data Security Review and Site Visit Summary


California Tribal Epidemiology Center
California Rural Indian Health Board, Inc.

# Data Security Review

This report highlights results of a discussion about data security on September 24, 2019 at CTEC. Vanesccia Cressi requested a review of current procedures to identify strengths and opportunities in CTEC data security practices. Tables throughout this report highlight data security categories, guidelines, evidence (in-person responses), and notes. Established guidelines and recommendations outlined in this report are intended to prevent data security breaches, minimize threats, promote secure data storage and access practices, explore data transmission and sharing practices, and describe data destruction practices.

September 24, 2019

**Recommended Citation:**
California Tribal Epidemiology Center. *Data Security Review and Site Visit Findings*. California Rural Indian Health Board, Inc. Roseville, CA. 2019

**Contact:**
The California Tribal Epidemiology Center
California Rural Indian Health Board, Inc.
1020 Sundown Way
Roseville, CA 95661
epicenter@crihb.org
916-929-9761

# Table of Contents

## Background

Data security is a growing concern in health care organizations and health information management. A study from 2015 reported that more than 750 data breaches occurred in the last year exposing 193 million personal records to potential for fraud and identity theft.[1] Of the 750 big data breaches, the top three were in the health care industry. Major breaches exposed names, birth dates, Social Security numbers, home addresses, and other personal information.[2] Data breaches of protected health information (PHI) occur most frequently through the use of a portable electronic device or laptop (32.7%), paper (22.3%), other media (18.8%), desktop/email (15.6%), and network servers (10.6). Data breaches involving PHI are most often the result of theft (58.2%), external vendor involvement (28.8%), and unauthorized access or disclosure (14.8%).[2] Experts report the best way to prevent a data security breaches is to design, implement, and test data security training for individuals and organizations that deal with data.

Data security involves several focus areas; these include:

1. Minimizing data security threats
2. Examining data storage and access practices
3. Data transmission and sharing practices
4. Personal device security
5. Erasing data
6. Data security plan


[1] Health Informatics (2019). *Why Data Security is the Biggest Concern of Health Care*. www.healthinformatics.uic.edu

[2] Liu, V., Musen, M. A., & Chou, T. (2015). *Data breaches of protected health information in the United States*. JAMA, 313(14), 1471-1473.

## Methods

To understand more about CTEC's data security plan and processes, the CTEC team (comprised of 10-12 CTEC staff, one consultant, one director, one deputy director, and one IT professional) reviewed data security guidelines and discussed what policies, procedures, or processes are in place. For each guideline the team discussed evidence and the consultant marked the level of evidence using a scale of Yes, No, and Not sure. The consultant recorded notes about the kinds of evidence provided or follow-up necessary to further support data security. Recommendations are included after the tables when appropriate and highlighted by a blue arrow.

## Results

The next sections highlight data security guidelines and findings from CTEC discussions.

## Minimizing Data Security Threats

| Guidelines | Evidence | Notes |
|---|---|---|
| **Evidence that CTEC acquires and handles only the minimum amount of sensitive data necessary?** | Yes | CTEC requests data without personally identifiable information. Only CTEC staff that need sensitive data have access to it via a Citrix shared file. CTEC requests that data is stripped of sensitive information prior to transmission. |
| **Evidence that CTEC provides data security training to new and existing employees annually.** | Yes | CTEC provides an annual security training for all employees and new employees complete several security training modules provided through I.H.S.[3] and Collaborative Institutional Training Initiative (CITI).[4] CTEC also requires HIPPA training and a local IT training for all employees. There was some discussion that not all employees take this training annually. |
| **Evidence that CTEC separates Personally Identifiable Information (PII) from all other data?** | Yes | CTEC has several practices in place that separate PII from other data. These practices are discussed throughout this report. |
| **Is PII stored, analyzed, and transmitted separately?** | Yes | CTEC uses a data protect file on the server that is only available to certain CTEC staff that require access. Another example is staff separate PII from other data received and stores data in a separate / locked compartment where data cannot be linked to PII. |
| **Are identifiers encrypted?** | Yes | IT staff indicated that CTEC uses Citrix to encrypt all identifiers. |
| **Evidence that paper-based surveys remove PII?** | Yes | CTEC staff assign unique identifiers to paper-based surveys. When this is not possible due to attrition, staff remove PII from paper-based surveys and store information in a separate secure file. |

[3] Indian Health Service Training. Available from: https://www.ihs.gov/issa/
[4] Collaborative Institutional Training Initiative. Available from: https://about.citiprogram.org/en/homepage/

### Recommendations on Data Security Threats

CTEC appears to have processes in place to minimize security threats. Continued efforts are needed to ensure storage, analysis, and transmission separates PII and does not include any PII. CTEC works with partners from Indian Health Service and organizations like CITI to ensure that staff have access to relevant training. These partnerships should continue. IT staff provide on-site training and support when questions arise, and this practice is an important one to minimize data security threats.

## Data Storage and Access

| Guidelines | Evidence | Notes |
|---|---|---|
| **Device-level encryption. Evidence that files require password upon start up, remote wiping capabilities in event of loss or theft.** | Yes | IT staff can remotely wipe any devices. IT uses Crypt Zone and other programs to encrypt sensitive data. |
| **Cloud Storage. Evidence that files are secure and comply with HIPPA** | N/A | CTEC does not use cloud storage and it is discouraged. In the event staff require use of Clouds, they are directed to comply with HIPPA and not transmit PII. |
| **Folder-level encryption. File-level encryption. IT-Administered Options.** | Yes | CTEC has a variety of folder and file level encryption options. Email files can be encrypted with clicking just one button on the email form. The data protect file is also encrypted. |
| **Server. Off-site access via Virtual Private Network. Two types of authentication.** | N/A | CTEC does not use a VPN. Staff may check out laptops with approval from the Director. These laptops have unique user and passwords for a predetermined time. |

### Recommendations on Data Storage and Access

Train staff on alternative approaches to cloud-based data sharing. Regularly educate staff on how to encrypt emails and files.

## Data Transmission and Sharing

| Guidelines | Evidence | Notes |
|---|---|---|
| **Secure Shell File Transfer Protocol (SFTP), including Secure Shell (SSH) or Secure Copy (SCP).** | Unsure | IT was not available during the discussion of this guideline, follow-up discussions regarding file transfer protocols may be necessary. |
| **Support for uploading an encrypted file to Dropbox or Box.** | No | IT does not recommend the use of Drop Box. IT provides support and encryption directions when uploading files for transmission/sharing. |
| **Emailing an encrypted file and sharing the password separately and securely. Mailing encrypted files loaded onto encrypted devices.** | Yes | CTEC has several processes in place that ensure emails with sensitive information are encrypted and passwords are sent separately and securely. All staff are trained on this during their orientation and routinely after. |

| | | |
|---|---|---|
| **Survey software with encryption features, such as SurveyCTO, that supports encryption during data collection and transmission to a central server.** | Unsure | CTEC uses a variety of survey software and discussion about the best online survey software included Qualtrics. It is recommended that staff use Qualtrics because it uses a Transport Layer Security (TLS) encryption for all transmitted data. Surveys can be protected with passwords and HTTP referrer checking. Data are independently stored and audited using the industry standard method (SSAE-16). |

### Recommendations on Data Transmission and Sharing

Data transmission and sharing procedures appear to follow recommended guidelines. Follow-up with the IT staff regarding secure transfer protocols is needed to respond to the first guideline. Additional conversations about the use of survey software like Qualtrics is also needed.

## Communication and Data Sharing with Partners

| Guidelines | Evidence | Notes |
|---|---|---|
| **Sharing data and receiving updates.** | Yes | CTEC has a data management plan and data security protocol that outlines data sharing and updates. |
| **Verifying data set does not contain unauthorized information prior to downloading, if possible.** | Yes | CTEC requests data without unauthorized information. For example, with death certificate data tribes black-out any PII. For missing files, CTEC uses up to four non-PII indicators to match individuals with death records. CTEC also met with legal teams about data sharing, access, and ensuring that unauthorized information is not included. |
| **Timeline for reviewing new data for unauthorized information or PII.** | Yes | CTEC has a data destruction policy that follows federal guidelines. In most cases this is seven years. A Chief Compliance Officer helps enforce timelines and reviews new data with PII. CTEC performs regular audits of new data. |
| **Notifying the source of the breach and requesting corrective action to prevent future breaches.** | Unsure | CTEC did not indicate there had been instances of a data breach. CTEC should follow the HIPPA 60-day reporting rule for any data breaches that occur. CTEC should ensure there is a notification process in place if and when a breach occurs involving non-HIPPA data. |
| **How files with unauthorized information will be removed and destroyed.** | Yes | IT destroys files with unauthorized information. Staff receive training on how to permanently delete files (double delete in email and trash). |

### Recommendations on Communication and Data Sharing

Sharing data among CTEC staff and with partners requires continued vigilance of data security protocols. There was less discussion about who to notify if a data breach occurs and corrective actions that would be taken to address the breach. It was unclear who is responsible for reviewing new data that comes into CTEC that may have unauthorized information or PII. A Chief Compliance Officer may conduct these duties, but in the event this position is vacant, this duty should be reassigned to

another staff member. This is particularly important with physical data (surveys, transcripts, photos, other qualitative data, CD-rom, thumb drive, etc.). One recommendation that came from this review was to create a log of all physical data received at CTEC. This log could be stored on the network, see Appendix A for an example data log.

## Personal Device Security

| Guidelines | Evidence | Notes |
|---|---|---|
| **CTEC uses a password-locked screensaver and timeout lock.** | Yes | IT programs all devices to lockout after 10 minutes. Individuals may change this on their individual computers. Deputy Director Kathleen Jack indicated that most data management plans indicate lockout after 5 minutes. |
| **CTEC uses a firewall.** | Yes | IT indicated all systems have firewalls. |
| **CTEC keeps all software up to date.** | Yes | IT indicated that all software is up to date. |
| **CTEC staff do not install or run programs from untrusted sources.** | Yes | CTEC staff are not able to install or run programs without administrator access. If staff need a specific software program, they first get approval from the Director and IT purchases the software and installs it for staff. |

### Recommendations on Personal Device Security

Routine education about personal device security will minimize threats. IT and staff should coordinate lockout times for consistency. Continued coordination and approval for software program installation with the IT department will ensure that programs from untrusted sources are not downloaded.

## Password Policies

| Guidelines | Evidence | Notes |
|---|---|---|
| **CTEC staff use strong passwords. Be at least eight characters, but preferably much longer. Not contain words, symbols for letter, person's name sequential letters or numbers.** | Yes | CTEC requires the use of strong passwords that are changed every 90-days. |

### Recommendations on Password Policies

Continue to require staff to change passwords every 90-days and never write passwords down next to their computers. Educate new employees on this practice.

## Preventing Data Loss

| Guidelines | Evidence | Notes |
|---|---|---|
| **CTEC backs up data regularly in two separate locations and passwords are retained for access.** | Yes | IT indicated that CTEC uses a back-up server. Two clinics store EHRs data. These are secured with strong passwords, encrypted, and access is limited. |

## Erasing Data

| Guidelines | Evidence | Notes |
|---|---|---|
| **Evidence of guidelines and actions that indicate data must be retained or destroyed when no longer needed. IRB or data provider may indicate this as well.** | Yes | Data management plans indicate retention and destruction practices. IRB applications indicate this as well. CTEC follows federal, date, or funding agency guidelines for data retention/destruction. |

## Conclusion

CTEC requested a review of data security procedures to discuss current data security practices and how to minimize threats and protected PII. Results of this review indicate that CTEC practices are consistent with recommended guidelines. Evidence to support these practices, processes, and training are outlined throughout this report. CTEC demonstrates a high-level of capacity to store, transmit, and share data using advanced encryption techniques. One of the many strengths of the CTEC data security process is the presence and support of the CRIHB IT team. IT works closely with CTEC Directors and staff to ensure that data security training and data security procedures are followed. Next steps may include following up on the recommendations outlined in this report and identifying an individual to lead data security efforts in the absence of a Chief Compliance Officer. Efforts to update data management plans and data security protocols in grant and IRB applications will provide consistency and shared understanding about data security. Future topics regarding data may include data preservation, data curation, and archiving. [5]

Working in partnership with tribes and community partners, CTEC's data security process is vital to retaining and protecting information and knowledge that will improve the health and wellbeing of current and future generations.

[5] For examples visit Iowa State University Data Management Plan. Available from: https://instr.iastate.libguides.com/dmp/step5

## Definitions

**Data Management Plan.** A plan developed by CTEC that outlines how data will be treated, stored, protected, retained, and destroyed.

**Data Use Agreement.** A contractual document used for the transfer of data that has been developed by nonprofit, government or private industry, where the data is nonpublic or is otherwise subject to some restrictions on its use.

**Electronic protected health information (ePHI).** This refers to PHI that is created, stored, transmitted, or received electronically.

**Family Educational Rights and Privacy Act (FERPA).** Educational data may be subject to the Family Educational Rights and Privacy Act (FERPA), which has special rules to protect the privacy of student records. FERPA may have implications for how researchers conduct evaluations and report results as related to obtaining individual consent from study participants.

**Health Insurance Portability and Accountability Act (HIPAA).** HIPAA provides regulation for healthcare data security, holding health care providers, insurance providers, researchers and others accountable for safeguarding protected health information (PHI) in the United States. Compliance requirements differ based on the party, such as individuals, covered entities, or researchers; the purpose of the data usage; and on stipulations or structure of data use agreements.

**HIPPA Data Breach.** This is an impermissible use or disclosure that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity can show there is a low probability the PHI has been compromised based on a risk assessment of at least the following four factors.[6]

**Protected Health Information (PHI).** Individually identifiable information reported by entities (health plans and clinicians) covered under the Health Insurance Portability and Accountability Act.

**Personally Identifiable Information (PII).** PII is any piece of information or combination of information that can be used to identify an individual with a reasonable amount of certainty. Examples: A Social Security number on its own is PII. An age, gender, and location combination may or may not be PII, depending on the age and size of the geographic area. “A 35-year-old man in Boston, MA” is not PII, but “A woman in her 90s in Chinook MT” is PII.

## Notes

This checklist was developed using the J-PAL Data Security Procedures for Researchers Guide developed by O’Toole, Feeney, Heard, and Naimpally August 2018. This document is intended to serve as a guide for CTEC as they develop and implement data security procedures. Professional data security firms and consultants may have additional resources and findings not included in this review.

Dr. Thomas McCoy (sub-consultant) was contacted via email on 9/25/19 to determine which survey software is the “best” and most secure. He recommended Qualtrics.

[6] Health and Human Services (ND). Breach Notification Rule. Available from: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

# Appendix A
## Physical Data Log Example

| | Date Received | Addressed To and From | Description of Data* | Storage Location | Sensitive Info/PII? | Notes Retention/Destruction |
|---|---|---|---|---|---|---|
| 1. | | | | | | |
| 2. | | | | | | |
| 3. | | | | | | |
| 4. | | | | | | |
| 5. | | | | | | |
| 6. | | | | | | |

*May include paper, CD-ROM, thumb drive, photos, other. This could be created in electronic and hard copy/paper format.

For more information about this report, contact:
Vanesscia Cresci, MSW, MPA
Research and Public Health Director
California Rural Indian Health Board, Inc.
1020 Sundown Way
Roseville, CA 95661
(916) 929-9761

vcresci@crihb.org